Industrial Internet of Things security modelling using ontological methods

JARWAR, Muhammad Aslam <http://orcid.org/0000-0002-5332-1698>, WATSON, Jeremy, ANI, Uchenna Daniel and CHALMERS, Stuarts

Industrial Internet of Things Security Modelling using Ontological Methods

Muhammad Aslam Jarwar
Sheffield Hallam University, Sheffield, UK
a.jarwar@shu.ac.uk

Jeremy Watson CBE FREng
University College London, London, UK
jeremy.watson@ucl.ac.uk

Uchenna Daniel Ani
Keele University, Keele, UK
u.d.ani@keele.ac.uk

Stuart Chalmers
National Physical Laboratory, London, UK
stuart.chalmers@npl.co.uk

ABSTRACT

The Industrial Internet of Things (IIoT) trend presents many significant benefits for improving industrial operations. However, its emergence from the convergence of legacy Industrial Control Systems (ICS) and Information and Communication Technologies (ICT) has introduced newer security issues such as weak or lack of end-to-end security. These challenges have weakened the interest of many critical infrastructure industries in adopting IIoT-enabled systems. Implementing security in IIoT is challenging because this involves many heterogeneous Information Technology (IT) and Operational Technology (OT) devices and complex interactions with humans, and the environments in which these are operated and monitored. This article presents the initial results of the PETRAS Secure Ontologies for Internet of Things Systems (SOfIoTS) project, which consists of key security concepts and a modular design of a base security ontology, which supports security knowledge representation and analysis of IIoT security.

KEYWORDS

Security attributes, Security ontology, Industrial Internet of Things, Cyber physical systems, Knowledge modelling

1 INTRODUCTION

The Internet of Things (IoT) supports applications that makes the lives of consumers easier and more convenient. The Industrial Internet of Things (IIoT) focuses on improved efficiency in operations and safety in production or process facilities, while in Building Management Systems (BMS), it is covering climate change effects. From an architectural view, the key differences between IoT and IIoT is the variation in types of services functionality requirements at the service layer. Currently, there is no common definition for IIoT, however, in this paper, we define IIoT as "*a system comprising networked smart objects, cyber-physical assets, associated generic information technologies and optional cloud or edge computing platforms, which enable real-time, intelligent, and autonomous access, collection, analysis, communications, and exchange of process, product and/or service information, within the industrial environment*" [18]. IoT and IIoT applications have become increasingly prevalent in the last decade and IoT device usage is growing exponentially [42]. Due to the rapid growth of IoT devices, development, and deployment complexities, most IoT/IIoT devices lack in-built security, which makes the systems attractive attack targets [25]. Thus, highly critical buildings, citizen services and industries are reluctant to adopt IIoT. For example, consider the level of damage and impact, which can occur due to security breaches and failure of IIoT applications that manage water treatment and reserve facilities (e.g., dams), autonomous rail networks, autonomous traffic signals, food chillers, energy supply systems, and supply chains [2, 36, 39]. These security issues stem from the integration of legacy Industrial Control Systems (ICS) with IoT and IIoT devices to enable improved functionality, productivity, and performance, leading to a wider threat landscape and introducing newer attack paths for targeting industrial systems.

The security of IIoT is challenging for several reasons. Firstly, it is unsafe to perform security audits or apply untested security solutions on live industrial systems. Live testing and security audit can disrupt the normal functioning of a system and potentially lead to disastrous consequences if the tested system consist of IIoT-enabled Critical National Infrastructures (CNIs). Secondly, most existing security solutions require resources such as memory, processing power, and storage, which is largely limited in current IoT/IIoT device technologies. Thus, security modelling (and simulations) is considered a viable alternative to enabling a capability to test security solutions on small-scale replica controlled-environment systems. However, modelling for IIoT systems is still challenging compared to IoT applications because IIoT applications consist of a large number of heterogeneous devices installed, and often distributed across a wider and multiple (remote) geographical locations. Also, IIoT devices involve other complex environmental factors such as the way the devices are operated, monitored, connected, and serviced, all of which are yet to be well-understood enough to inform appropriate security solutions.

Ontological methods are one of the recognised and acceptable approaches for structuring the knowledge of such complex environments in other application domains (e.g. Banking, Tourism, Biomedical repository management, clinical diagnosis, Social IoT) [12, 31–33, 41]. Semantic ontological methods are already prevalent in IoT applications for virtualisation and representation of sensor attributes and observations. Example of these methods include W3C Semantic Sensor Network Ontology (SSN) , OneM2M and Web of Things (WoT) [10, 21**?**]. There are also examples where ontologies have been explored for security purposes, for instance, threat modelling and appropriate countermeasures, intrusion detection, Internet of Medical Things (IoMT) security assessment, and Web of Things security modelling [8, 13, 23, 40]. However, these ontological methods are application-specific and follow dissimilar approaches, thus lacking the flow for a common standardised ontological view that is applicable to modeling cybersecurity and

applies to IIoT systems and related network components with a focus on cascading effects and security goals. The benefits of using ontologies for modelling the security of IIoT are threefold: **(1)** Helping to define the essential concepts, terms, rules and knowledge base to support the security of IIoT according to a set of security goals, **(2)** Enabling and supporting the capability to (re)share and (re)use security knowledge bases and models across multiple applications in similar domains to drive common understanding and interoperability, **(3)** Inferring (with appropriate reasoning engines) additional security concepts, relations as well as risks.

Based on the aforementioned challenges and benefits of using ontological methods, our paper introduces the secure ontology for IIoT environments. We present initial results, which include key security concepts and a modular approach to develop a base ontology for modelling the security of IIoT. Moreover, we aim to provide an ontological analysis of key security concepts that could help in modelling the critical IIoT environment's security in case of failure of IoT devices due to cyber-attack. In this paper, concepts, terms, and classes are used as synonyms to describe IIoT devices' security knowledge. Additionally, in this work and to explain our approach, the term 'security' is used to imply 'cybersecurity'.

The rest of the paper is structured as follows. Section 2 provides a literature review. Section 3 provides an overview of the SOfIoTS approach to modelling security of IIoT systems. Section 4 presents security domain knowledge and a base ontology. Section 5 concludes the paper.

2 RELATED WORK

The W3C WoT working group recently released the Web of Things Security Ontology (WoTSO) for cross-domain interoperable security modelling [8]. The WoTSO contains 9 classes, 6 object properties, and 8 data properties. Among them, the *'SecurityScheme'* is the main class, and has 8 subclasses and relevant object and data properties such as "name" and "in". In WoTSO, some security schemes could also be combined with other schemes, where there is a higher risk of threats to IIoT devices. The combination of multiple security schemes is important, as it provides an additional security layer and makes it difficult for malicious threat agents to access devices. For example, various biometric signatures and multifactor authentication schemes can be combined to authenticate legitimate users and for granting access to IoT devices and networks. Authorization, token, and proxy are considered the prominent properties used to identify the Uniform Resource Identifie (URI) of an authentication server, URI of a token server, and URI of a proxy server respectively. The WoTSO is not a partially generalised ontology because it describes some related concepts at an instance level. It includes classes and properties provided with clear definitions and sufficient metadata, so they can be extended independently. The WoTSO concepts are not aligned with the 8 security goals defined in [3] and do not support them, for example, availability, safety, resiliency, and utility. The *'SecurityScheme'* class is similar to *'SecurityMechanism'* class, which was previously proposed in [27].

The IoT Security Ontology (IoTSO) was developed based on ISO/IEC 13335-1:2004 guidelines for components risk analysis, the National Institute of Standards and Technology (NIST) Special Publication 800-12 for information security and by identifying and considering the information security issues from the existing literature [17, 27**?**]. The IoTSO centered on the analysis of relations among security risk components. It contains Asset, Threat, Vulnerability, Security Mechanism, Security Property and Type of Defense concept. In IoTSO, network components, connections and IoT devices were represented with an 'Asset' class and system attacks that compromise and/or damage the asset were modelled with the 'Threat' class. The 'Vulnerability' class represents the metadata for any kind of weaknesses that poses the risk of attack [**?**], 'SecurityMechanism' class represents security approaches to protect the assets. Similarly, 'TypeOfDefense' class has been used to identify the type of defense that should be applied. For example, active attack detection, passive attack detection, and attack prevention. The links among the classes could be established through several object properties. For instance, the 'hasVulnerability' property could be applied to Asset and Vulnerability classes, and 'isSecurityMechanismOf' property has been used to create a link between a threat and security mechanism. IoTSO was used to model the security of IoT systems at design time and runtime [26]. The design time modelling provides the security services to business process and application-level security, while runtime security is aligned to monitoring and actuating of IoT devices from the industrial access and controls units. The IoTSO based framework was also developed for adaptive security features and decision-making in industry[28]. The adaptive features were learned from the environment and used to prevent, identify, and respond to malicious cyber-attacks at runtime [28]. In IoTSO, the classes and properties were defined generally, therefore, these can be extended for further knowledge representation in the IIoT domain. The Web Ontology Language (OWL) version of IoTSO can be accessed from the GitHub page[1].

Alanen et al., 2022 [11] developed a Hybrid Reliability, Availability, Maintainability, Safety, and Security (HRAMSS) risk assessment management ontology and an associated Security Threat Analysis Methodlogy (STAM) with an ICS use case. To develop the ontology, a comparison of security risk assessment in ICS and OT was investigated. The authors argue that conflict between security and safety directly relates to the availability of processes and services, and availability can be minimized to save the infrastructure from potential cyber-attacks. However, if safety functions require continuous processes and services availability, then availability related system components (e.g., network communications, network devices) should have the higher priority of protection. To balance the security, safety and availability of systems in the industrial domain, authors proposed 4 core concepts: Imperfection, HRAMSS, Risk Control, and Negative Impact. The Imperfection contains Fault and Vulnerability concepts; Hazard, Loss scenario and Threat concepts are classified into HRAMSS hazard category; Risk control category is further sub-categorized into *ProtectiveMeasure*, *ImprovementMeasure*, and *CounterMeasure* concepts; the Negative impact category is unbundled with Harm, Loss, and Impact concepts. The HRAMSS ontology can be extended for cybersecurity risk assessment in IIoT environments, as it provides sufficient metadata and related classes

[1]https://github.com/brunomozza/IoTSecurityOntology/blob/master/iotsec.owl (accessed Jan. 19, 2022)

[11]. The HRAMSS ontology contains similar concepts and properties to other ontologies. For example, the vulnerability and threat attributes were also proposed in IoTSO and WoTSO [8, 27].

3 SECURE ONTOLOGIES FOR IIOT SYSTEMS

The SOfIoTS project objective is to develop a base security ontology that provides sufficient metadata and allows the creation of subclasses or equivalent classes and relationships to model the security of IIoT and/or their Digital Twins Infrastructure (DTS). Fig:1 shows the illustration of SOfIoTS ontology approach, where SOfIoTS classes (in blue color) are reused and extended by the PETRAS[2] projects such as Security of Centralized Transport Infrastructure Efficiency System (ISCTIES) , Processes for Securing for Water Resource Management Systems (PSWaRMS), Cognitive and Socio-Technical Cybersecurity in Modern Railway System (CoSTCMoRS), Modelling for Socio-technical Security (MASS) [4–7]. The SOfIoTS ontology supports both IT and Operational Technology OT components of IIoT. In SOfIoTS, the modular approach is followed to develop and evaluate the ontology, so that concepts and properties should be self-contained, having clarity and supporting reusable knowledge. The concepts in the SOfIoTS ontology also focus on security goals along with four system constituent domains: people, process, physical, and technical. This is on the premise that IIoT systems do not only comprise technology and processes, but also include people using the technology and the environment where both the people and technologies operate [14]. All four constituents are involved in a system of relations and interactions to enable the proper functioning and security of the IIoT system. To follow the modular approach, SOfIoTS categorises classes into prevention, detection, and response to the attack. Typically, the latter includes correction and recovery. The advantages of SOfIoTS approach are threefold: **(1)** Supporting improved sharing and reusability of security domain knowledge, which is important for holistic end-to-end security modelling of integrated OT and IT components. **(2)** Complementing machine learning models with domain knowledge data and metadata[3] to facilitate inferencing and localisation of security issues and the selection of appropriate countermeasures. . **(3)** Supporting scalability by adding more IT and OT components and enabling the structuring of data and metadata related to security requirements such as dynamic or contextual permission for accessing of IoT devices and their data.

4 BASE ONTOLOGY FOR IIOT SECURITY

4.1 Ontology Development Methodology

There is no standard way for developing ontologies. However, a well-defined ontology can be realised through an iterative process, which include: **(1)** determining the scope of ontology, **(2)** considering reusing the classes from the existing ontologies, **(3)** writing down important terms, **(4)** defining the classes and classes hierarchy and **(5)** defining properties for classes [30]. In order to develop a security ontology for IIoT, we considered the existing theories and best practices, including Bunge's ontological theory, Stanford ontology development guide, Mentor methodology and NeOn Methodology [19, 30, 34, 37]. The mentor methodology proposed a two phase process for developing an enterprise reference ontology: **Phase 1** contains terminology gathering, glossary building, thesaurus building, and **Phase 2** focuses on the reusing of existing domain knowledge through ontologies gathering, harmonization and mapping [34]. The NeOn methodology offers 9 different scenarios for an ontology development, including starting from scratch through to several levels of reusing, re-engineering and merging [37]. According to Bunge's ontological theory, the conceptual model for anything can be represented with things, properties, attributes, events, states, systems and the interactions among them [19]. The properties are intrinsic to Things[4] and Things can be modelled as functional schema represented with properties and attributes. Things can move from one state to another, for example, static permissioning mechanism can be changed to dynamic or contextual. Our paper combined the concepts and methodologies from [19, 30, 34, 37], which considered most appropriate for SOfIoTS approach and applicable to the scope of four projects: ISCTIES, PSWaRMS, CoSTCMoRS, MASS [4–7] and uses cases in ICS and CNIs.

Building on the idea from [19], our approach posits that a conceptual model of a system can be built with things, properties, and their associations with other things. For instance, the association among legacy machines, IoT devices, network components, and humans. Learning from [30], we adopted a step-by-step process for developing a secure ontology. Also, from [34], we learned that common concepts and properties enabled and improved the understandability among various parties e.g., different IIoT projects and their applications.

The horizontal and vertical is a stratification of ontologies for structuring and representing the knowledge of things. Both horizontal and vertical approaches have pros and cons. The horizontal approach negatively impacts the structural simplicity, increases number of objects, and broadens the ontological choices. In the vertical stratified approach, the structural simplicity of ontology is improved as it reduces the number of objects due to the generalisation of concepts. The SOfIoTS approach uses common concepts with abstract definition by following the vertical as well as horizontal stratification. From [37], our approach adopted the reusing and reengineering of ontological[5] as well as non-ontological resources[6] methodology, which improves the reusability and extendibility of ontologies and reducing the research and development time. In SOfIoTS ontology development, concepts and properties are reused/mined from ontological and non-ontological resources. For example, the definitions for various concepts are informed from the Industrial Internet Consortium Security Framework (IICSF) [35] (which is a non-ontological resource) and the concept of Attack is reused from the IoT Network Security Situation Awarenes (INSSA) ontology [43].

[2]Petras - Home." https://petras-iot.org/ (accessed Apr. 12, 2022)

[3]For example, Domain knowledge (DK) is necessary for choosing the best data for a countermeasure machine learning system. The security ontology concepts, attributes, and transitive and intransitive relations (i.e., data and metadata) are used to model the DK.

[4]In IIoT Things can represent smart grids, robots, connected vehicles, sensors, actuators, network components and cloud servers

[5]The ontological resources consists of well-defined structured datasets, however each attribute in the dataset must be in a relationship with one or many other attributes within the same datasets such as in SSN and IoTSO.

[6]The non-ontological resources consists of structured datasets (e.g., IIoT security dataset [9]) as well unstructured data (e.g., academic and newspaper articles).

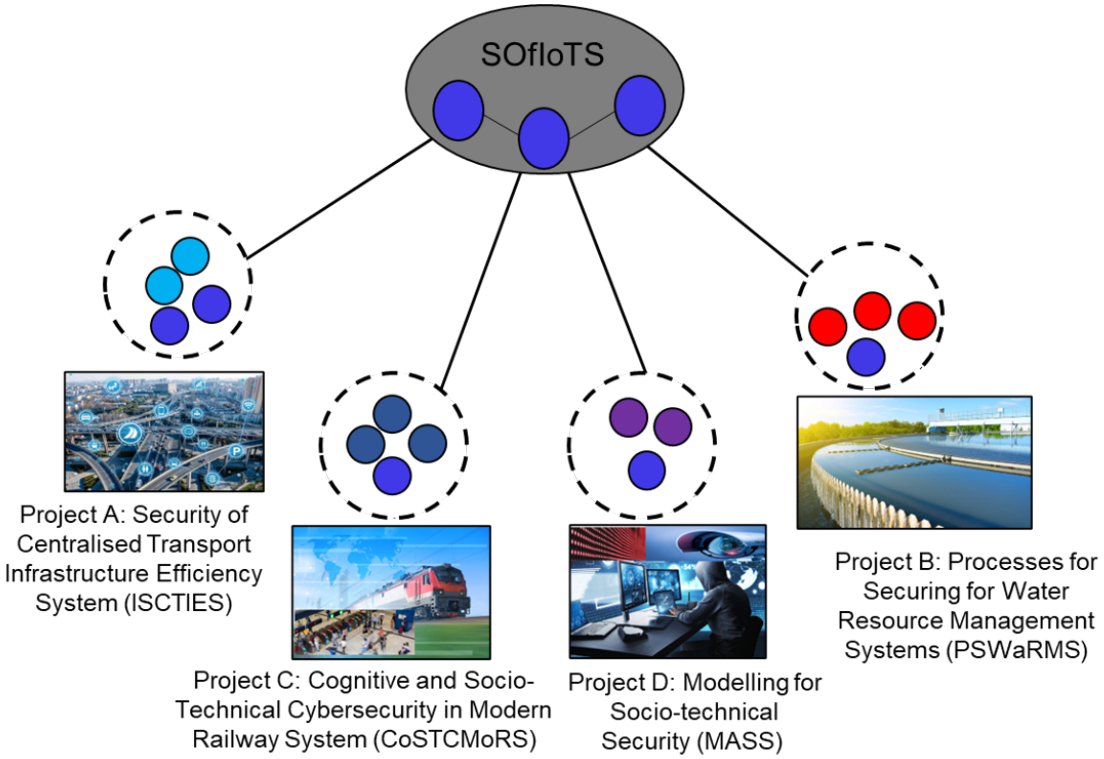

Figure 1: Secure Ontologies for IoT Systems (SOfIoTS) approach

4.2 Concepts in Secure Ontology

The conceptual model[7] of the SOfIoTS ontology is presented in Fig:2, showing the classes, properties, and their relationships.

The SOfIoTS ontology contains 9 classes and 18 object properties, among them some classes have been reused from the existing security ontologies. The primary concepts in SOfIoTS ontology include Asset, Attack, Fault, *SecurityGoal*, *SecurityMechanism* and Vulnerability. The Capability, Criticality, and Risk are classified as secondary concepts. Each concept is defined as follows:

i **Asset:** Asset is the most common term which is used in many security ontologies. Jbair et al. [24] defines asset as "*Industrial Cyber-Physical Systems (ICPS) components and services that threat actors aim to compromise*". The Asset can represent configuration in IT and OT, software, hardware, or integrated subsystems, which can be impacted by vulnerabilities. The asset could be used to protect other components in the IIoT ecosystem through developing a security mechanisms and tools. [35]. Asset is a more abstract term and is suitable for use in a base security ontology instead of *Product* and *Technology* terms which were used in prior security ontologies [38]. Humans are also part of the IIoT system, and the human operators and users can also be classified as assets as these humans interact with and use hardware, software, and integrated subsystem to perform the task. Humans can also have vulnerabilities that can be exploited and impacted by internal and external vulnerabilities, along with other system components.

ii **Attack:** The Attack concept is drawn from INSSA ontology [43]. Some authors have used Attack term instead of Threat. For SOfIoTS base ontology, we define the Attack concept as the metadata that characterises an unlawful action or set of unlawful actions against any of the IIoT assets that impact enterprise entities and leads to endangering the safety, availability, integrity, confidentiality, accountability, productivity, and reputation of organisations and/or their operations. The Attack concept represents both active and passive attacks. The active attacks can directly disturb and interrupt IIoT devices which could hamper availability, integrity, and safety. On the other hand, a passive attack could be more harmful to confidentiality and privacy in Consumer IoT (CIoT) and secrecy in IIoT. The information gained through passive attacks could be used in the future for opportunistic attacks. To identify and perform reasoning for advanced security knowledge such as the impact, risk, and capability of an attacker, the attack class is semantically linked to other classes such as Vulnerability and *SecurityGoal* (as shown in Fig:2).

iii **Capability:** The Capability concept represents metadata and data about the quality, strength, or state of skills in terms of cyber-attacks and security mechanisms. The Capability concept's data and metadata provide answers to questions about

[7]The conceptual model refers to building a formal representation of a phenomenon or system pertaining to the real world and it is used to understand or simulate a system.

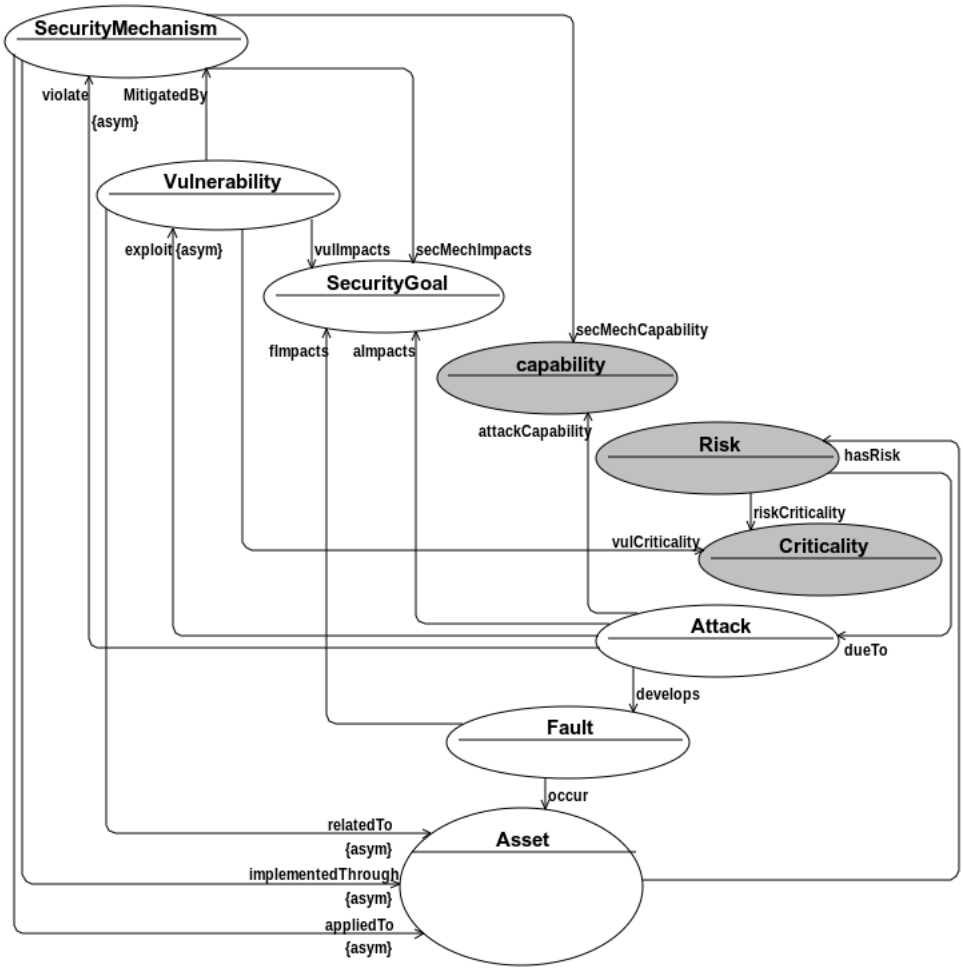

Figure 2: Conceptual model for SOfIoTS ontology; secondary concepts are marked with gray color

the active or passive state of an attack. It can also help to indicate whether an attack has the capability to impact (control and/or suspend) the functions of IoT devices, or it just monitors the exchange of data such as in an eavesdropping attack, or it can add spoofing sensor or actuator device in the network for illegitimate advantage by exploiting the Constrained Application Protocol (COAP). In SOfIoTS ontology, the Capability class has asymmetric relationship[8] with the Attack and *SecurityMechanism* classes.

iv **Criticality:** In SOfIoTS ontology, the criticality concept is similar to the capability concept, however, it is mostly used to represent a negative sense and is a synonym for 'Severity' or *SeverityScale* as in [27]. Thus, the criticality concept characterises the criticality of devices with respect to a potential vulnerability and risk. The criticality data could be determined through the potential scale of damage to the critical system or infrastructure,

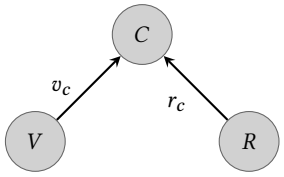

Figure 3: Criticality class (C) with associated classes Vulnerability (V) and Risk (R) and object properties *vulCriticality* (vc) and *riskCriticality* (rc)

the attack impact on the assets, and security goals (i.e., confidentiality, availability, integrity, safety, resilience). In SOfIoTS ontology, the Criticality class has a relationship with the Vulnerability and Risk classes through *riskCriticality* and *vulCriticality* properties as shown in Fig:3, where node represents the class and edge annotation implies the property or relationship.

[8]Asymmetric relationship asserts that the Attack and SecurityMechanism instances can be associated with the capability class attributes. Nevertheless, the Capability class is restricted from that association.

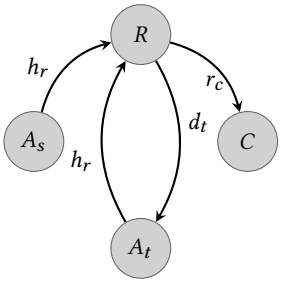

Figure 4: Risk class (R) with associated classes Asset (A_s), Attack (A_t), Criticality (C) and properties *hasRisk* (hr), *riskCriticality* (rc) and *dueTo* (d_t)

v **Fault** The Fault concept is informed by ideas from [11, 15]. A fault is a trigger, which may lead to a failure. The Fault concept represents the incapable or limited characteristics of things, machine, sensor, actuator, and smart grid. It also includes security mechanisms which restrict things from performing functions for which they have been built. The industrial faults normally occur due to prior presence of security vulnerabilities, impact of cyber-attacks, wear and tear, malicious agents, incompetence, and lack of security knowledge. Additionally, a fault concept can represent wear and tear of assets that could be the reason for the emergence of a vulnerability and/or a breach of security mechanisms. In SOfIoTS ontology, the 'Fault' class has a relationship with the Attack, Asset, and *SecurityGoal* classes through "develops", "occur" and "impacts" properties, respectively.

vi **Risk:** The Risk concept is drawn from [11, 35]. In industrial safety engineering, risk characterises the probability of harm, whereas in cybersecurity, risk represents the likelihood of a negative impact on assets due to potential threat or successful cyber-attack on a known security vulnerability assuming the weak or absent security control. In SOfIoTS ontology, the risk concept is used to determine and represent the likelihood of attacks and their cascading impacts on assets and security goals. The risk has criticality, and the greater the risk criticality the greater impact of attack on assets and security goals, and also the greater the requirement for sophisticated security mechanisms. In SOfIoTS ontology, the Risk has relationships with other classes, for instance Criticality, Attack, and Asset.The graphical representation of Risk class relationships with other classes is shown in Fig: 4.

vii **SecurityGoal:** The SecurityGoal concept characterises security parameters that ensure the protection of assets and interest of stakeholders. Additionally, SecurityGoal concept's data and metadata might be used to assess how well the available security controls are able to protect assets of interest. There are 8 security goals, which are used to represent different purposes [3]. For example, availability, resilience, and safety are used to assess the continuity of services, and the safety of people and assets. Integrity, utility, and authenticity focus on data/information security, the trustworthiness of security controls, devices and machines. Confidentiality and Access control deals with disclosure of information to only authorised assets and/or things. There are also various factors that impact security goals. For instance, vulnerability and fault in the relevant assets, capability of available security mechanisms in response to an attack. In SOfIoTS ontology, the *SecurityGoal* class has relationships with other classes (see in Fig:2) which support the affinity analysis of IIoT security.

viii **SecurityMechanism:** The SecurityMechanism concept is derived from [22]. It characterises the practices that protect IIoT devices from attacks and keeps them safe and unimpaired as designed and ensures availability, confidentiality, and integrity. The NIST 800-12 highlights that *SecurityControl*, Safeguard, and *CounterMeasure* are synonyms [**?**]. We believe that Safeguard, countermeasure and SecurityControl can not truly represent security mechanisms in general, therefore, we have chosen the *SecurityMechanism* term for our base security ontology.

ix **Vulnerability:** The Vulnerability concept is adopted from the NIST Vulnerability Description Ontology (VDO), which defines vulnerability as a weakness in the system hardware, system internal controls, and codes [**?**]. According to IICSF, a vulnerability is a weakness in the system which oftenly used by the attackers for targeting the same asset or other connected assets [35]. In SOfIoTS, we define a vulnerability as the characteristics of a weakness in the targeted IIoT asset, either due to social or technical reasons or wear and tear, that the attacker could exploit to gain illegitimate rights or access.

4.3 Secure Ontology Implementation and Assessment

The excerpt view of ontology in Turtle syntax is shown in List 1 and the complete representation of implementation can be accessed from [1]. The Protégé and OWLGrEd[9] tools have been used for electronically generating and building the conceptual model into an RDF/XML format. In order to ensure that the SOfIoTS ontology meets the contents, structure, and other criteria of design and development, the developed ontology is assessed using four criteria i.e., clarity, consistency, conciseness, and completeness as described in [38]. The SOfIoTS ontology passed the 'clarity' criteria, because it provides enough metadata for each concept and formal and common terms have been chosen from cybersecurity domains. The SOfIoTS ontology supports 'consistency' features because all the classes are logically coherent, unambiguous, and semantically connected with other classes through object properties. As a base ontology, SOfIoTS ontology does not support the 'conciseness' feature because it has many properties. The rationale for including many properties is in part to consider and capture all possible relations and phenomenon of IIoT security. The SOfIoTS ontology supports the 'completeness' criteria as it includes sufficient classes and properties to represent the security of IIoT generally. It can be extended to develop a domain and application ontology for more localised features. For further work in this regard, we aim to assess the quality of the developed ontology through a survey or engagement with experts in the IIoT, cybersecurity and ontology, accordingly. Additionally, we aim to build enhancement in the security ontology, drawing from ensuing feedback and recommendations.

[9] http://owlgred.lumii.lv/ (accessed Apr. 27, 2022)

Listing 1: Excerpt view of SOfIoTs base ontology in Turtle syntax

```
owl:versionIRI <http://www.localhost.org/foo/ontologies/SOfIoTS/1.01> .
    :Asset rdf:type owl:Class .
    :Attack rdf:type owl:Class .
    :Criticality rdf:type owl:Class .
    :Fault rdf:type owl:Class .
    :Risk rdf:type owl:Class .
    :SecurityGoal rdf:type owl:Class .
    :SecurityMechanism rdf:type owl:Class .
    :Vulnerability rdf:type owl:Class .
    :capability rdf:type owl:Class .
    :MitigatedBy rdf:type owl:ObjectProperty ;
          rdfs:domain :Vulnerability ;
          rdfs:range :SecurityMechanism .
        :appliedTo rdf:type owl:ObjectProperty ,
                   owl:AsymmetricProperty ;
        rdfs:domain :SecurityMechanism ;
        rdfs:range :Asset .
```

5 CONCLUSION

This article presents an ontological approach to structure the cybersecurity of IIoT. The main contribution of this paper is that it showcases the relevant security concepts, their relations, and interdependence along security goals, faults, risks, and assets. In order to support the sharing and reusability of security ontology in many other PETRAS projects, a top-down approach and abstract terms from ontological and non-ontological resources have been followed in analysing and formalising the development. Moreover, by following the principle of clarity, each concept has been explained with proper definition and usage examples. It is believed that the proposed ontological approach will further develop research foci and fill knowledge gaps in structuring cybersecurity knowledge for IIoT-enabled critical infrastructure systems. Future work includes exploring the continuous development of the proposed ontology and work to expand the knowledge base with relevant insights. Also to explore the assessment and evaluation of the efficacy of the proposed security ontology through survey and engagement with experts in IIoT, ontologies and cybersecurity.

ACKNOWLEDGMENTS

This work has been supported by the PETRAS National Center of Excellence in IoT Systems Cybersecurity, which is funded by the UK EPSRC under grant number EP/S035362/1.

REFERENCES

[1] [n. d.]. Secure Ontologies for IoT Systems (SOfIoTS) -Ontology. https://bit.ly/3xteq2I. accessed on :2022-06-08.
[2] [n. d.]. Advanced Persistent Threat. https://bit.ly/3mt8iBm. accessed on: 2022-01-11.
[3] [n. d.]. Code of Practice: Cyber Security in the Built Environment – revised second edition. https://electrical.theiet.org/guidance-codes-of-practice/publications-by-category/cyber-security/code-of-practice-cyber-security-in-the-built-environment-revised-second-edition/
[4] [n. d.]. Petras - Cognitive and Socio-Technical Cybersecurity in Modern Railway System. https://bit.ly/3zvbNip. accessed on: 2022-04-12.
[5] [n. d.]. Petras - Improving the Security of Centralised Transport Infrastructure Efficiency System. https://bit.ly/3H4HSiB. accessed on: 2022-04-12.
[6] [n. d.]. Petras - Modelling for Socio-technical Security. https://bit.ly/3H3Vn1V. accessed on: 2022-04-12.
[7] [n. d.]. Petras - Processes for Securing for Water Resource Management Systems. https://bit.ly/3zqmQcD. accessed on: 2022-04-12.
[8] [n. d.]. Web of Things (WoT) Security Ontology. https://www.w3.org/2019/wot/security. Last Accessed:2021-12-18.
[9] [n. d.]. WUSTL-IIOT-2021 Dataset for IIoT Cybersecurity Research. http://www.cse.wustl.edu/~jain/iiot2/index.html. accessed on :2022-10-18.
[10] 2016. *TS 118 112 - V2.0.0 - oneM2M; Base Ontology (oneM2M TS-0012 version 2.0.0 Release 2)*. Technical Report.
[11] Jarmo Alanen, Joonas Linnosmaa, Timo Malm, Nikolaos Papakonstantinou, Toni Ahonen, Eetu Heikkilä, and Risto Tiusanen. 2022. Hybrid ontology for safety, security, and dependability risk assessments and Security Threat Analysis (STA) method for industrial control systems. *Reliability Engineering & System Safety* 220 (2022), 108270. https://doi.org/10.1016/j.ress.2021.108270
[12] Sajjad Ali, Muhammad Golam Kibria, Muhammad Aslam Jarwar, Hoon Ki Lee, and Ilyoung Chong. 2018. A Model of Socially Connected Web Objects for IoT Applications. *Wireless Communications and Mobile Computing* 2018 (2018). https://doi.org/10.1155/2018/6309509
[13] Faisal Alsubaei, Abdullah Abuhussein, Vivek Shandilya, and Sajjan Shiva. 2019. IoMT-SAF: Internet of Medical Things Security Assessment Framework. *Internet of Things* 8 (2019), 100123. https://doi.org/10.1016/j.iot.2019.100123
[14] Uchenna P Daniel Ani, Hongmei He, and Ashutosh Tiwari. 2017. Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective. *Journal of Cyber Security Technology* 1, 1 (2017), 32–74.
[15] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr. 2004. Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing* 1, 1 (2004), 11–33. https://doi.org/10.1109/TDSC.2004.2
[29]]VDO Harold Booth and Christopher Turner. [n. d.]. NIST- Vulnerability Description Ontology (VDO). http://csrc.nist.gov/publications. accessed on :2022-04-11.
[17] Pauline Bowen, Pauline Bowen, Joan Hash, and Mark Wilson. 2007. Information Security Handbook: A Guide for Managers. *NIST SPECIAL PUBLICATION 800-100, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY* (2007), 178—-800. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.697.168
[18] Hugh Boyes, Bil Hallaq, Joe Cunningham, and Tim Watson. 2018. The industrial internet of things (IIoT): An analysis framework. *Computers in Industry* 101 (2018), 1–12. https://doi.org/10.1016/j.compind.2018.04.015
[19] Mario Bunge. 1977. *Treatise on basic philosophy: Ontology I: the furniture of the world*. Vol. 3. Springer Science & Business Media.
[29]]Charpenay Victor Charpenay, Sebastian Käbisch, and Harald Kosch. [n. d.]. Introducing Thing Descriptions and Interactions: An Ontology for the Web of Things. ([n. d.]). http://purl.oclc.org/net/unis/OWL-IoT-S.owl
[21] Michael Compton, Payam Barnaghi, Luis Bermudez, Raúl García-Castro, Oscar Corcho, Simon Cox, John Graybeal, Manfred Hauswirth, Cory Henson, Arthur Herzog, Vincent Huang, Krzysztof Janowicz, W. David Kelsey, Danh Le Phuoc, Laurent Lefort, Myriam Leggieri, Holger Neuhaus, Andriy Nikolov, Kevin Page, Alexandre Passant, Amit Sheth, and Kerry Taylor. 2012. The SSN ontology of the W3C semantic sensor network incubator group. *Journal of Web Semantics* 17 (2012), 25–32. https://doi.org/10.1016/j.websem.2012.05.003
[22] Amelie Gyrard, Christian Bonnet, and Karima Boudaoud. 2014. An Ontology-Based Approach for Helping to Secure the ETSI Machine-to-Machine Architecture. In *2014 IEEE International Conference on Internet of Things (iThings), and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom)*. 109–116. https://doi.org/10.1109/iThings.2014.25
[23] Almut Herzog, Nahid Shahmehri, and Claudiu Duma. 1. An Ontology of Information Security. *https://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/jisp.2007100101* 1, 4 (jan 1), 1–23. https://doi.org/10.4018/JISP.2007100101
[24] Mohammad Jbair, Bilal Ahmad, Carsten Maple, and Robert Harrison. 2022. Threat modelling for industrial cyber physical systems in the era of smart manufacturing. *Computers in Industry* 137 (may 2022), 103611. https://doi.org/10.1016/J.COMPIND.2022.103611
[25] Kenneth Kimani, Vitalice Oduol, and Kibet Langat. 2019. Cyber security challenges for IoT-based smart grid networks. *International Journal of Critical Infrastructure Protection* 25 (2019), 36–49. https://doi.org/10.1016/j.ijcip.2019.01.001
[26] Bruno Augusti Mozzaquatro, Carlos Agostinho, Joao Goncalves Diogo, Martins, and Ricardo Jardim-Goncalves. 2018. An Ontology-Based Cybersecurity Framework for the Internet of Things. *SENSORS* 18, 9 (2018). https://doi.org/10.3390/s18093053
[27] Bruno A. Mozzaquatro, Ricardo Jardim-Goncalves, and Carlos Agostinho. 2015. Towards a reference ontology for security in the Internet of Things. In *2015 IEEE International Workshop on Measurements Networking (M N)*. 1–6. https://doi.org/10.1109/IWMN.2015.7322984
[28] Bruno A Mozzaquatro, Raquel Melo, Carlos Agostinho, and Ricardo Jardim-Goncalves. 2016. An ontology-based security framework for decision-making in industrial systems. In *2016 4th International Conference on Model-Driven Engineering and Software Development (MODELSWARD)*. 779–788.
[29]]Nieles Michael Nieles, Kelley Dempsey, and Victoria Yan Pillitteri. [n. d.]. NIST Special Publication 800-12 Revision 1 An Introduction to Information Security. https://doi.org/10.6028/NIST.SP.800-12r1. https://doi.org/10.6028/NIST.SP.800-

12r1

[30] Natalya F Noy, Deborah L McGuinness, and Others. 2001. Ontology development 101: A guide to creating your first ontology.

[31] Alejandro Rodríguez-González, Ángel García-Crespo, Ricardo Colomo-Palacios, Fernando Guldrís Iglesias, and Juan Miguel Gómez-Berbís. 2011. CAST: Using neural networks to improve trading systems based on technical analysis by means of the RSI financial indicator. *Expert Systems with Applications* 38, 9 (sep 2011), 11489–11500. https://doi.org/10.1016/J.ESWA.2011.03.023

[32] Alejandro Rodríguez-González, Jose Emilio Labra-Gayo, Ricardo Colomo-Palacios, Miguel A. Mayer, Juan Miguel Gómez-Berbís, and Angel García-Crespo. 2012. SeDeLo: Using semantics and description logics to support aided clinical diagnosis. *Journal of Medical Systems* 36, 4 (aug 2012), 2471–2481. https://doi.org/10.1007/S10916-011-9714-1/TABLES/3

[33] María Del Pilar Salas-Zárate, Rafael Valencia-García, Antonio Ruiz-Martínez, and Ricardo Colomo-Palacios. 2016. Feature-based opinion mining in financial news: An ontology-driven approach:. *http://dx.doi.org/10.1177/0165551516645528* 43, 4 (may 2016), 458–479. https://doi.org/10.1177/0165551516645528

[34] Joao Sarraipa, Joao P M A Silva, Ricardo Jardim-Goncalves, and Antonio A C Monteiro. 2008. MENTOR — A methodology for enterprise reference ontology development. In *2008 4th International IEEE Conference Intelligent Systems*, Vol. 1. 6–40. https://doi.org/10.1109/IS.2008.4670436

[35] Sven Schrecker, Hamed Soroush, Jesus Molina, Jeff Caldwell, David Meltzer, Frederick Hirsch, Jean Pierre Leblanc, and Marcellus Buchheit. 2016. Industrial Internet of Things Volume G4: Security Framework. (2016).

[36] Ioannis Stellios, Panayiotis Kotzanikolaou, Mihalis Psarakis, Cristina Alcaraz, and Javier Lopez. 2018. A Survey of IoT-Enabled Cyberattacks: Assessing Attack Paths to Critical Infrastructures and Services. *IEEE Communications Surveys & Tutorials* 20, 4 (2018), 3453–3495. https://doi.org/10.1109/COMST.2018.2855563

[37] Mari Carmen Suárez-Figueroa, Asunción Gómez-Pérez, and Mariano Fernández-López. 2012. The NeOn methodology for ontology engineering. In *Ontology engineering in a networked world*. Springer, 9–34.

[38] Romilla Syed. 2020. Cybersecurity vulnerability management: A conceptual ontology and cyber intelligence alert system. *Information & Management* 57, 6 (2020), 103334. https://doi.org/10.1016/j.im.2020.103334

[39] Nilufer Tuptuk, Peter Hazell, Jeremy Watson, and Stephen Hailes. 2021. A systematic review of the state of cyber-security in water systems. *Water* 13, 1 (2021), 81.

[40] Jeffrey Undercoffer, Anupam Joshi, and John Pinkston. 2003. Modeling Computer Attacks: An Ontology for Intrusion Detection. In *Recent Advances in Intrusion Detection*, Giovanni Vigna, Christopher Kruegel, and Erland Jonsson (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 113–135.

[41] Rafael Valencia-García, Francisco García-Sánchez, Dagoberto Castellanos-Nieves, and Jesualdo Tomás Fernández-Breis. 2011. OWLPath: An OWL ontology-guided query editor. *IEEE Transactions on Systems, Man, and Cybernetics Part A:Systems and Humans* 41, 1 (jan 2011), 121–136. https://doi.org/10.1109/TSMCA.2010.2048029

[42] Christos Xenofontos, Ioannis Zografopoulos, Charalambos Konstantinou, Alireza Jolfaei, Muhammad Khurram Khan, and Kim-Kwang Raymond Choo. 2022. Consumer, Commercial, and Industrial IoT (In)Security: Attack Taxonomy and Case Studies. *IEEE Internet of Things Journal* 9, 1 (2022), 199–221. https://doi.org/10.1109/JIOT.2021.3079916

[43] Guangquan Xu, Yan Cao, Yuanyuan Ren, Xiaohong Li, and Zhiyong Feng. 2017. Network Security Situation Awareness Based on Semantic Ontology and User-Defined Rules for Internet of Things. *IEEE Access* 5 (2017), 21046–21056. https://doi.org/10.1109/ACCESS.2017.2734681