Industrial Internet of Things Security Modelling using Ontological Methods

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

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

Jeremy Watson CBE FREng
University College London, London, UK
jeremy.watson@ucl.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 new 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 (SoIoTS) 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 is 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 IIoT/IoT 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 SOIoTS approach to modelling 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 ‘isSecurityMechanism’ 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.

Alalen et al., 2022 [11] developed a Hybrid Reliability, Availability, Maintainability, Safety, and Security (HRAMSS) risk assessment management ontology and an associated Security Threat Analysis Methodology (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 and Negative Impact contains CounterMeasure concepts; the Negative impact category is further sub-categorized into ProtectiveMeasure, ImprovementMeasure, and CounterMeasure concepts; the HRAMSS ontology can be extended for cybersecurity risk assessment in IIoT environments, as it provides sufficient metadata and related classes

---

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 PE-TRAS 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 the understanding of machine learning models with domain knowledge data and metadata 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 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 onto logical 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 Awareness (INSSA) ontology [43].


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.

IoT2022, November 07–10, 2022, Delft, The Netherlands
4.2 Concepts in Secure Ontology

The conceptual model\(^7\) of the SOfloTS ontology is presented in Fig:2, showing the classes, properties, and their relationships.

The SOfloTS ontology contains 9 classes and 18 object properties, among them some classes have been reused from the existing security ontologies. The primary concepts in SOfloTS 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 SOfloTS 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.
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 SOFloTS ontology, the Capability class has asymmetric relationship\(^8\) with the Attack and SecurityMechanism classes.

iv Criticality: In SOFloTS 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,\(^8\) 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.

---

\(^8\)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 2: Conceptual model for SOFloTS ontology; secondary concepts are marked with gray color

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 SOFloTS 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.
v Fault: The Fault concept is informed from ideas [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 SOIoTS 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 SOIoTS 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 the impact of attack on assets and security goals, and also the greater the requirement for sophisticated security mechanisms. In SOIoTS ontology, the Risk has relationships with other classes, for instance Criticality, Attack, and Asset. The graphical representation of Risk class relationships with other classes (see in Fig: 2) which support the affinity analysis of IIoT security.

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 SOIoTS 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 and ensures availability, confidentiality, and integrity. The NIST 800-12 highlights that SecurityControl, Safeguard, and Countermeasure are synonyms [27]. 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 [27]. According to IICS, 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 SOIoTS, 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 tools have been used for electronically generating and building the conceptual model into an RDF/XML format. In order to ensure that the SOIoTS 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 SOIoTS 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 SOIoTS 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, SOIoTS 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 SOIoTS 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.

---

9http://owlgred.lumii.lv/ (accessed Apr. 27, 2022)
5 CONCLUSION

This article presents an ontological approach to structure the cybersecurity of IoT. 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 and fill knowledge gaps in structuring cybersecurity knowledge for IoT. The main contribution of this paper is that it presents an ontological approach to structure the cybersecurity of IIoT. The main contribution of this paper is that it presents an ontological approach to structure the cybersecurity of IIoT.

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

[29] [Nielen Michael Nielen, Kelley Dempsey, and Victoria Yan Püllitteri. [n. d.]. NIST Special Publication 800-12 Revision 1 An Introduction to Information Security. https://doi.org/10.6028/NIST.SP.800-


