Computers in Industry 101 (2018) 1–12

Contents lists available at ScienceDirect

Computers in Industry

journal homepage: www.elsevier.com/locate/compind

The industrial internet of things (IIoT): An analysis framework

Hugh Boyes*, Bil Hallaq, Joe Cunningham, Tim Watson

Cyber Security Centre, WMG, University of Warwick, Coventry, CV4 7AL, UK

ARTICLE INFO

Keywords:
Industrial internet of things
Cyber-physical systems
Industry 4.0
IIoT
IACS

ABSTRACT

Historically, Industrial Automation and Control Systems (IACS) were largely isolated from conventional digital networks such as enterprise ICT environments. Where connectivity was required, a zoned architecture was adopted, with firewalls and/or demilitarized zones used to protect the core control system components. The adoption and deployment of 'Internet of Things' (IoT) technologies is leading to architectural changes to IACS, including greater connectivity to industrial systems. This paper reviews what is meant by Industrial IoT (IIoT) and relationships to concepts such as cyber-physical systems and Industry 4.0. The paper develops a definition of IIoT and analyses related partial IoT taxonomies. It develops an analysis framework for IIoT that can be used to enumerate and characterise IIoT devices when studying system architectures and analysing security threats and vulnerabilities. The paper concludes by identifying some gaps in the literature.

1. Introduction

The concept of Industrial Automation and Control Systems (IACS) is well established. These systems, often referred to as Operational Technology (OT), are employed in diverse industries including manufacturing, transportation and utilities, and are sometimes referred to as cyber-physical systems (CPS). Since the term Internet of Things (IoT) [1] was first used in 1999, it has been applied to connected devices in consumer, domestic, business and industrial settings [2]. Although there is a significant amount of literature attempting to define IoT, its uses, and its typical components, it is rarely made obvious how any of this applies in the industrial setting.

Because current definitions of IoT invariably imply a similar approach to the high-level architecture of a system, the ubiquitous use of the term IoT to refer to the use of digital technologies in industry is unhelpful as it hinders the analysis of alternative system architectures, including the location and nature of the data or information processing, and associated performance and security issues. The aims of this paper are to improve on existing definitions of Industrial IoT (IIoT) and to propose a framework for IIoT components as a basis for analysing the use and deployment of IoT technologies in industrial settings. In undertaking this research our aim was to establish a framework that allows us to analyse the nature of IIoT devices and their uses, which is to be used as part of a vulnerability and threat analysis process for these devices. By being able to characterise the devices in a systematic manner, we anticipate being able to analyse cross-cutting threats and vulnerabilities and identify patterns that may be obscured when focusing on the technology employed or sector specific issues.

This paper is structured as follows: Section 2 provides some further background to CPS, IACS, and the Industrial Internet, setting it against the background of Industry 4.0. Section 3 provides our analysis and definition of IIoT, which builds on existing explanations that are presented. Section 4 presents our framework. Finally, Section 5 identifies gaps in the current literature that need to be addressed in future work

2. Background

Whilst researching IIoT we have reviewed a wide range of academic literature and found that when combining the search terms:

> ("Industrial Machines" OR "Industrial Systems") AND "Internet" OR ("Industrial Internet") AND "Machines"

The following terms were amongst those most regularly found:

> Cyber Physical Systems (CPS), Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA), and Industrial Internet.

Although not an exhaustive list, it does represent the most commonly used terms in both academic and relevant non-academic literature, for white papers and corporate blogs. In the rest of this section we define Industry 4.0 and review the above terms before moving on to develop our definition of IIoT and the taxonomy.

* Corresponding author.
E-mail address: hb@warwick.ac.uk (H. Boyes).

https://doi.org/10.1016/j.compind.2018.04.015
Received 7 December 2017; Received in revised form 21 March 2018; Accepted 20 April 2018

2.1. Industry 4.0

The first three industrial revolutions are characterised as being driven by mechanical production relying on water and steam power, use of mass labour and electrical energy, and the use of electronic, automated production respectively [3]. Whilst the supposed fourth industrial revolution ('Industry 4.0') was first proposed in 2011 in the context of the goal of developing the German economy [4]. This revolution is characterised by its reliance on the use of CPS capable of communication with one another and of making autonomous, de-centralised decisions, with the aim of increasing industrial efficiency, productivity, safety, and transparency.

There is a considerable overlap between the concept of Industry 4.0 developed in Germany and the Industrial Internet concept (see 2.6), which originated in the United States. The definition of the latter now encompasses change for both business and individuals:

> "…the industrial internet is an internet of things, machines, computers and people enabling intelligent industrial operations using advanced data analytics for transformational business outcomes, and it is redefining the landscape for business and individuals alike" [5].

A definition of 'Industrie 4.0′ a term which, in its English cognate, the authors treat as synonymous with IIoT, is:

> "…we define Industrie 4.0 as follows: Industrie 4.0 is a collective term for technologies and concepts of value chain organisation. Within the modular structured Smart Factories of Industrie 4.0, CPS monitor physical processes, create a virtual copy of the physical world and make decentralized decisions. Over the IoT, CPS communicate and cooperate with each other and humans in real time. Via the IoS [Internet of Services], both internal and cross- organizational services are offered and utilised by participants of the value chain." [6]

2.2. Cyber-physical systems (CPS)

Whilst there are a number of definitions of CPS [7–11], this paper uses: "A system comprising a set of interacting physical and digital components, which may be centralised or distributed, that provides a combination of sensing, control, computation and networking functions, to influence outcomes in the real world through physical processes." [12]

What sets CPS apart from more conventional information and communications systems (IT or ICT) is the real-time character of their interactions with the physical world. Whilst both CPS and ICT systems process data and/or information, the focus of CPS is on the control of physical processes. CPS use sensors to receive information about, including measurements of, physical parameters, and actuators to engage in control over physical processes. CPS often involve a large degree of autonomy. For example, CPS often have the capacity to determine whether to change the state of an actuator or to draw a human operator's attention to some feature of the environment being sensed.

2.3. Industrial automation & control systems (IACS)

IACS or ICS is a collective term typically used to describe different types of control systems and associated instrumentation, which include the devices, systems, networks, and controls used to operate and/or automate industrial processes. Descriptions of ICS from authoritative American and European organisations are respectively:

- "Initially, ICS had little resemblance to traditional information technology (IT) systems in that ICS were isolated systems running proprietary control protocols using specialized hardware and software. Many ICS components were in physically secured areas and the components were not connected to IT networks or systems. Widely available, low-cost Internet Protocol (IP) devices are now replacing proprietary solutions" [13]; and
- "Today ICS products are mostly based on standard embedded systems platforms, applied in various devices, such as routers or cable modems, and they often use commercial off-the shelf software" and "command and control networks and systems designed to support industrial processes. The largest subgroup of ICS is SCADA" [14].

2.4. Supervisory control and data acquisition (SCADA)

SCADA has been described as:

- A system that allows an operator, in a location central to a widely distributed process, such as an oil or gas field, pipeline system, or hydroelectric generating complex, to make set point changes on distant process controllers, to open or close valves or switches, to monitor alarms, and to gather measurement information [15];
- Similar to a Distributed Control System with the exception of sub-control systems being geographically dispersed over large areas and accessed using Remote Terminal Servers [16]. Where a Distributed Control System (DCS) is a supervisory control system typically controls and monitors set points to sub-controllers distributed geographically throughout a factory [17]; and
- SCADA applications are made up of two elements: the process/system/machinery you want to monitor and control, which can take the form of a power plant, a water system, a network or a system of traffic lights; and a network of intelligent devices that interface with the first system through sensors and control outputs. This network, which is the platform system, provides the capability to measure and control specific elements of the first system [18].

The nature of SCADA has led to conflicting views as to whether it forms part of the IIoT ecosystem. For example, discussion of SCADA system forensic analysis within IIoT [19] contrasts with a view that SCADA is simply the predecessor to IIoT especially as SCADA systems have evolved to connect to the internet but do not have the analytics and level of connectivity that is found in IIoT [20].

2.5. Industrial internet

The concept of an Industrial Internet was first articulated by General Electric (GE) [21], and described as:

> "The definition of the Industrial Internet includes two key components: The connection of industrial machine sensors and actuators to local processing and to the Internet; The onward connection to other important industrial networks that can independently generate value. The main difference between the consumer/social Internets and the Industrial Internet is in how and how much value is created. For consumer/social Internets, the majority of value is created from advertisements" [22].

This description clearly separates the Internet and the Industrial Internet, although in both cases the function of the Internet is to provide the wide area networking. More recently the Industrial Internet has been defined as:

> "… a source of both operational efficiency and innovation that is the outcome of a compelling recipe of technology developments [*sic*]. The resulting sum of those parts gives you the Industrial Internet—the tight integration of the physical and digital worlds. The Industrial Internet enables companies to use sensors, software, machine-to-machine learning and other technologies to gather and analyse data from physical objects or other large data streams—and then use those analyses to manage operations and in some cases to offer new, value-added services" [23].

From this definition, it is apparent that the authors consider a key component of the Industrial Internet to be the ability to analyse data, which is corroborated by a statement later in their report, in which it is stated that "⋯Big Data analytics is the foundation of the Industrial Internet…". This desire to collect and analyses data is a feature in common with Industry 4.0.

3. Industrial internet of things (IIoT)

Whilst there are numerous IoT definitions, those of relevance to industrial application make explicit the kinds of smart components that get embedded into ordinary objects so that those objects can count as IoT devices, and form constituents of cyber-physical systems (CPS). Three relevant definitions are:

- A definition for the IoT would be a "group of infrastructures, interconnecting connected objects and allowing their management, data mining and the access to data they generate" where connected objects are "sensor(s) and/or actuator(s) carrying out a specific function that are able to communicate with other equipment" [24];
- "The terms 'Internet of Things' and "IoT" refer broadly to the extension of network connectivity and computing capability to objects, devices, sensors, and items not ordinarily considered to be computers. These "smart objects" require minimal human intervention to generate, exchange, and consume data; they often feature connectivity to remote data collection, analysis, and management capabilities" [25]; and
- "The IoT represents a scenario in which every object or 'thing' is embedded with a sensor and is capable of automatically communicating its state with other objects and automated systems within the environment. Each object represents a node in a virtual network, continuously transmitting a large volume of data about itself and its surroundings…" [26].

On the basis of these, an initial definition of IIoT might be: the use of certain IoT technologies – certain kinds of smart objects within cyber-physical systems – in an industrial setting, for the promotion of goals distinctive to industry. Similar simple definitions were found in our literature search, for example:

- "The Industrial Internet of Things (IIoT) is the use of Internet of Things (IoT) technologies in manufacturing" [27]; and
- "Industrial Internet: A short-hand for the industrial applications of IoT, also known as the Industrial Internet of Things, or IIoT" [28].

Such a simple conception is not sufficient for our purposes in this paper, however. We need something substantive and a precise conception to inform our proposed IIoT framework. The simple conception does provide a template for a definition of IIoT, for it correctly attempts to define IIoT by appeal to two essential features: (a) the kinds of technologies that are used in an IIoT setting and (b) the distinctive aims and purposes to which those technologies are put. We need a definition which has that structure, but which gives us a more substantial expansion of (a) and (b).

An advantage of the simple conception is that because it makes it clear that the relevant technologies are used for purposes distinctive to industry, it satisfies the basic criterion of enabling us to distinguish IoT devices from IIoT devices. For example, devices such as smart bike locks and smart kettles are not useful from the point of view of industry *per se*, the simple conception correctly classifies those items as non-IIoT devices. Despite this advantage, the definition remains uninformative nevertheless.

A further pitfall to avoid when attempting to arrive at a definition of IIoT is defining IIoT in terms of some other notion, which is not obviously different from the notion of IIoT itself, which would render the definition uninformatively circular. That sort of problem is exemplified in the industry-driven literature by, for example:

> "The IIoT vision of the world is one where smart connected assets (the things) operate as part of a larger system or systems of systems that make up the smart manufacturing enterprise" [29].

Since 'smart manufacturing enterprise' is essentially an industrial enterprise that exemplifies the features of IIoT, this definition is also uninformatively circular.

In seeking to formulate an improved conception of IIoT we searched the contemporary academic and industry-driven literature for more informative definitions than those already cited. We found a few that improved on the simplistic and circular definitions already presented.

A definition that improves incrementally over the simple definition is:

> "Industrial Internet or Industrial Internet of Things (IIoT) is built for bigger 'things' than smartphones and wireless devices. It aims at connecting industrial assets, like engines, power grids and sensor to cloud over a network" [30].

This definition goes beyond the simple conception by making it explicit that it is industrial assets which are counted as connected in an IIoT setting, and it tells us a little about the nature of that connection: that the relevant assets are connected to a cloud, over a network.

A second definition which adds some further details is:

> "The Industrial Internet of Things (Industrial IoT) is made up of a multitude of devices connected by communications software. The resulting systems, and even the individual devices that comprise it, can monitor, collect, exchange, analyse, and instantly act on information to intelligently change their behaviour or their environment – all without human intervention" [31]

The central advantage of this still admittedly vague definition is that it makes it clear what the function of IIoT devices is: to monitor, collect, exchange, and analyse information so as to enable them to change their own behaviour, or else instruct other devices to do so, without human intervention.

A number of researchers writing in German, offer a cluster of definitions of IIoT that share a focus on the kinds of technologies which are put into operation in IIoT settings, and the ways they are put to use in those settings. It is suggested that a central element of IIoT is its reliance [32], in an industrial setting, on objects, systems and machinery which has been upgraded to the status of a CPS, so that products and services can be guided through the supply and value chains in an autonomous manner. Another perspective [33] is that IIoT relies not just on CPS, but also on embedded systems, cloud computing, edge computing, the generic technologies associated with the smart factory, and associated software. A further insight [34] relates to the aims and purposes of IIoT technologies, suggesting that they should not merely function to enable autonomous production, but enable real-time information to users, consumers and other processes. The definition of Industrie 4.0 in Section 2.1 sheds light on the kinds of technological processes utilised as part of IIoT, and how those processes are applied in promoting the values of the relevant industries whilst also making it explicit how IIoT technologies are connected to other features of the industrial technological landscape, such as Smart Factories and the Internet of Services (i.e. a "thing" as a service, e.g. Power as a Service or Mobility as a Service).

We are now able to provide our own working definition of IIoT. It has the same structure as the simple conception we started out with: IIoT is defined by appeal to the kinds of technologies which compose it, as well as by appeal to the distinctive uses to which those technologies are put, but builds in more details that the simple conception:

> *Industrial Internet of Things*: 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, so as to optimise overall production value. This value may include; improving product or service delivery, boosting productivity, reducing labour costs, reducing energy consumption, and reducing the build-to-order cycle.

4. IIoT: an analysis framework

Before developing our analysis framework, we reviewed existing published material on industry-focused IoT taxonomies and a range of industry material, in particular manufacturers' white papers, case studies and technical articles describing specific products or implementations. We identified seven published IoT taxonomies in the academic literature, which address the IoT as a whole and are not specifically focused on IIoT.

4.1. Review of existing IoT taxonomies

In undertaking this research our aim was to establish a framework that allows us to analyse the nature of IIoT devices and their uses, which is to be used as part of a vulnerability and threat analysis process for these devices. None of the taxonomies outlined above provide sufficient coverage of the characteristics of devices to support our objectives. The specific limitations of the taxonomies can be summarised as follows:

(a) the device-centric taxonomy [35] – this approach provides useful characteristics at device level (e.g. energy, communication, functional attributes, local interface, hardware and software resources), but does provide information about the role of the device, its physical or architectural locations, and the sector in which it is being used;

(b) the IoT stack-centric taxonomy [36] – whilst some of the characteristics (e.g. service, data, interaction and thing) addressed in this approach may be of value the stack does not relate to the conventional IACS hierarchy that is described in the Purdue Model [37]. We considered the concept of service in this taxonomy to be flawed as a particular device may contribute to fulfilment of multiple business objectives;

(c) the IoT sensor taxonomy [38] – the characteristics (e.g. motion, position, environment, mass measurement and biosensor) used by this approach are useful for devices that have a sensing capability, but this is only a subset of the range of IIoT devices;

(d) the IoT-based smart environment taxonomy [39] – this is of limited utility from a security perspective as its emphasis is on classification of the networking elements (e.g. communication enablers, network type, technologies, local area wireless standards, objectives and characteristics), the technology elements are very broad and the objectives (e.g. cost reduction) are difficult to apportion at device rather than system level;

(e) the IoT architecture taxonomy [40] – this combines a mixture of business architecture and technical characteristics (e.g. applications, enabling technologies, business objectives, architectural requirements, IoT platforms architecture types and network topologies), but given the use of only six classification elements is of limited value for classifying devices;

(f) the Industrial Internet of Things taxonomy [41] – the approach is immature in terms of the classification criteria (e.g. reliability, real-time, data item scale, module scale, runtime integration, distribution focus and collection focus) with only single examples given for each criterion, and the six criteria would not provide us with sufficient granularity to compare and contrast the security profile of individual devices;

(g) the domain or sector-based IoT taxonomies [42] – this is helpful in addressing the business use to which a device is being put, however this taxonomy does not address the technical or architectural aspects of device design and deployment as it identifies the type of device but not its characteristics.

Whilst none of the existing taxonomies meet our needs, as they are either too high level or incomplete from a device characterisation perspective, we can draw upon them and our own investigation of current IIoT proposed and actual solutions to develop an analytical framework for IIoT devices. We also considered the theoretical foundations of cyber manufacturing [43] and the work published by the CyPhERS project, for example [44]. However, neither of these publications provide the framework we were seeking as a basis for analysing devices.

Given the limitations in the published literature we have developed a framework for characterising IIoT devices. We have not sought to call it a taxonomy as it does not have a branching structure based on a single root, nor is it an ontology, given inconsistent use of many of the technology terms and the propensity for product marketers to create new jargon to differentiate their products.

Our approach, which is described in more detail below is to characterise devices based on six categories, with each category having a number of sub-categories:

- Industry sector;
- Device location;
- Connectivity;
- Device characteristics;
- Device technology;
- User type.

Each of the remaining sub-sections sets out the rational for including the category within our framework, providing a diagram that illustrates its breakdown and a rational for the proposed structure. In setting out our framework we provide examples of each category using a programmable logic controller (PLC) as the device.

4.2. Industry sector

The industry sectors illustrated in Fig. 1 are relevant to the severity and nature of threats to an organisation and the IIoT devices deployed in the organisation's operational systems [45]. All of the sectors make use of IACS to varying degrees, and there is likely to be increased use of IIoT based on industry trends reported by market research companies as referred to in Section 4.1. With the exception of retail, the sub-categories listed above are generally recognised as critical infrastructure of developed economies. Retail has been included to reflect the criticality of supply of essential supplies to citizens and to reflect the increasing technical complexity of many retail outlets, for example the building automation, management and security systems deployed in their premises. The breakdown of the Manufacturing sector is adapted from the report on digital manufacturing commissioned by the UK government [46].

Using this category the PLC might be described as:

$$\text{Industry Sector} \rightarrow \text{Electricity} \rightarrow \text{Transmission}.$$

4.3. Location

In Fig. 2, we propose a taxonomy that considers the location of the IIoT device from a number of perspectives, which are relevant in terms of the device's exposure to risks from both cyber and physical security perspectives.

Four sub-categories are proposed:

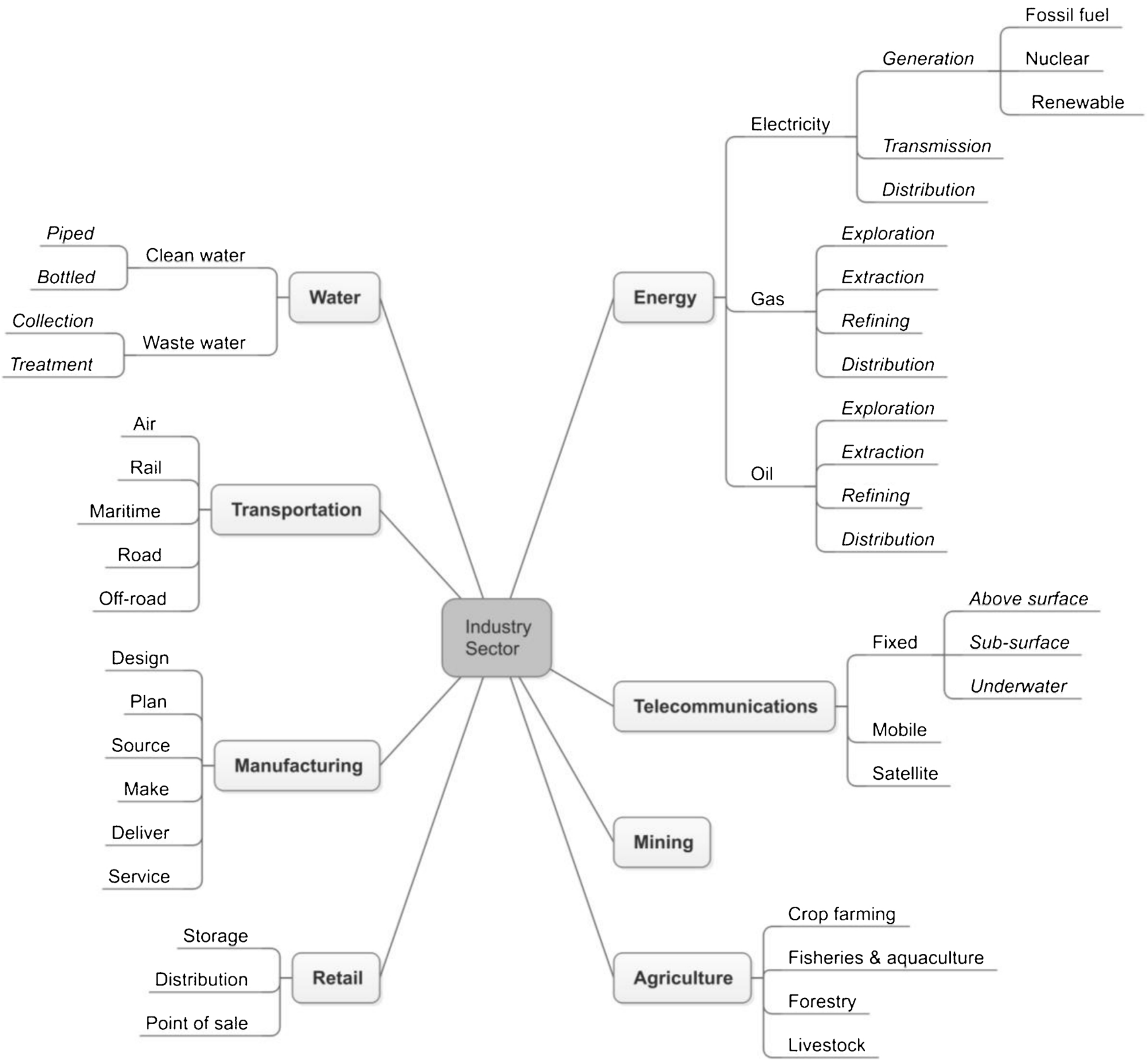

Fig. 1. Industry Sector category.

(a) Ecosystem – There are a number of models offered for IoT ecosystems [47–50], but these are generic and not specifically related to IIoT implementations. An ecosystem model that does directly related to industrial applications [51] is illustrated in Fig. 3. The proposed classification scheme is adapted from this model but extended to include the wider enterprise IT to accommodate the convergence of information and operation technologies, and adjacencies. In the Thing class we have included a sub-class “Monitor’ to accommodate devices that provide a wider functionality than measurements, e.g. a CTV camera.

(b) Purdue Model – the Purdue Model for Control Hierarchy [52,53] is a well-recognised model in the manufacturing industry that segments devices and equipment into hierarchical functions. This model has been used by international standards organisations [54,55] to specify a zone and conduit model for IACS security and is also used in a variety of security [56] and safety [57] guidance material. The model, illustrated in Fig. 4, uses the concept of zones in order to subdivide Enterprise and ICS networks into modules that function in a similar way.

(c) Physical – this element seeks to characterise the environment that the device is installed, which therefore allows the level of physical security vulnerability to be considered. For example, devices that are located externally are likely to be much more susceptible to physical damage, theft or being interfered with, as well as being exposed to the elements and a variety of natural hazards.

(d) Mobility – this element provides an indication of whether the device is only used in a fixed location or may be moved around, on its own or as part of a system. Mobile devices are likely to require a wireless communications mechanism to convey data and permit configuration and/or control, thus exposing the device to the threat of interference or jamming. In addition, there may be a need to track or geolocate the device so as to correctly interpret the data it provides.

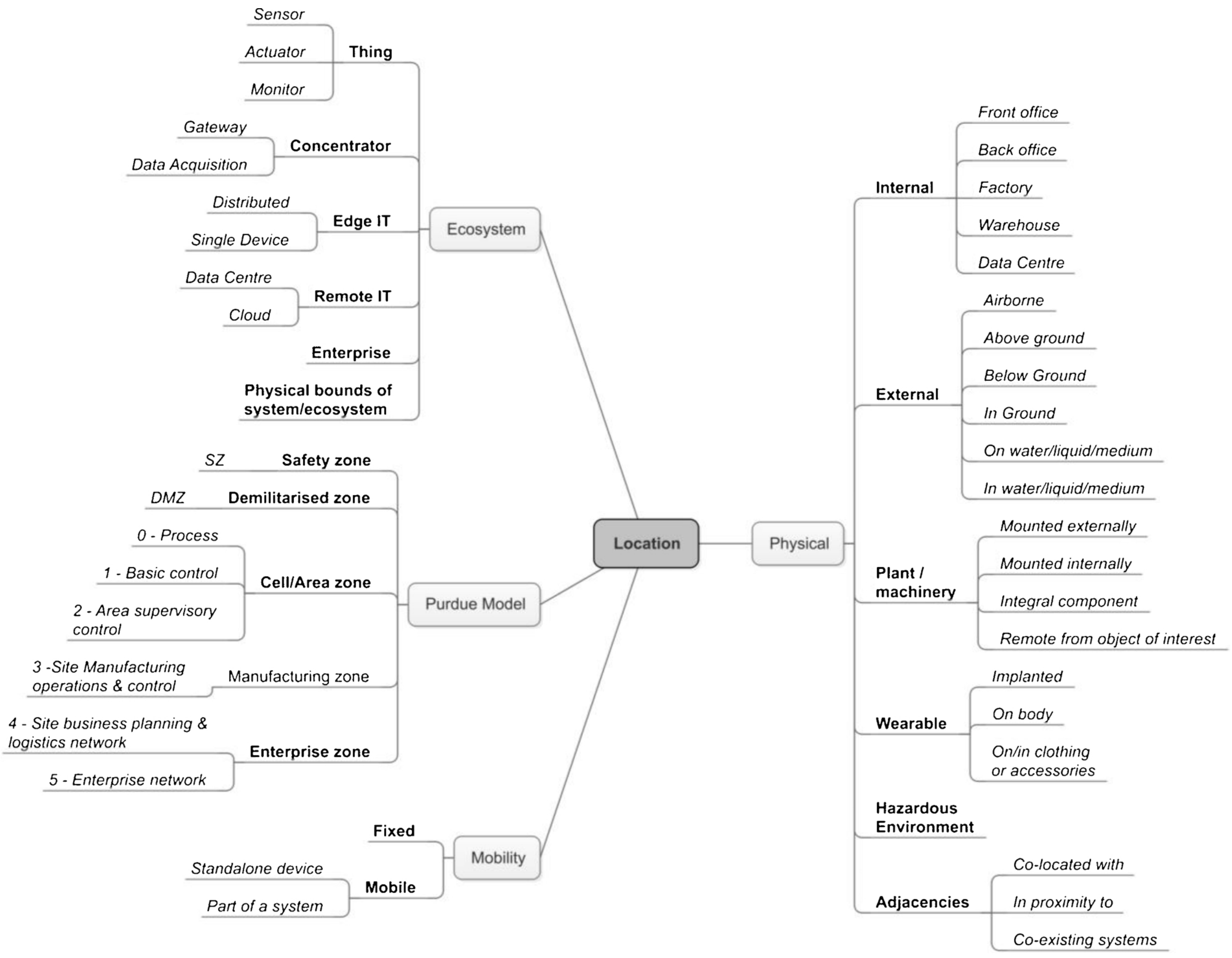

Fig. 2. Location category.

Using this category the PLC might be described as:

$$\begin{aligned}\text{Location} &\rightarrow \text{Ecosystem} \rightarrow \text{Concentrator} \rightarrow \text{Data acquisition}\\ &\rightarrow \text{Purdue Model} \rightarrow \text{Cell/Area zone} \rightarrow 1 - \text{Basic Control}\\ &\rightarrow \text{Physical} \rightarrow \text{External} \rightarrow \text{Above Ground}\\ &\rightarrow \text{Mobility} \rightarrow \text{Fixed}\end{aligned}$$

4.4. Connectivity

The proposed connectivity characteristics are illustrated in Fig. 5, the aim of using these is to identify the essential features of the networking or communications connectivity between the device and the IIoT system within which it operates.

The five proposed sub-categories are explained as follows:

(a) Mechanism – the focus of this sub-category is on the physical mechanism used to convey any communications to or from the device. Two classes that may appear unusual are no connectivity and physical connectivity. The former relates to devices that may be recording changes to the environment, where measurement data is stored in the device for later recovery on its retrieval and decommissioning, for example an IoT-based dosimeter. The latter relates to devices in hazardous or extreme environments, for example an IoT device employing ultrasonic communications rather than RF signals in an inflammable or explosive environment.
(b) Nature – whether the communications is in real-time or near real-time, implying continuous connectivity is required, or whether data can be stored and forwarded either on a schedule or on request.
(c) Initiation – this relates to how communication is initiated;
(d) Protocols – this relates to the protocols used to establish and manage the link and to convey information, examples of the three classes are: Infrastructure (IPv4, IPv6, 6LoWPAN, UDP); Discovery (mDNS, HyperCat, UPnP); and Data protocols (MQTT, XMPP, LLAP, REST, SOAP).
(e) Link security – this focuses on the level of security and trust involved in establishing and operating the connectivity.

Using this category, the PLC may be described as:

Connectivity → Mechanism → Wired → Electrical / electronic

→ Initiation → Either device

→ Protocols → Infrastructure → RS485

→ Protocols → Infrastructure → USB [Not in use]

→ Protocols → Data protocols → ModbusRTU

→ Link security → Authorization → Not required

→ Link security → Encrypted → None

4.5. Device characteristics

The focus of the proposed device characteristics, illustrated in Fig. 6, is on functionality of the device, specifically how important it is to the system it is part of, the function the device provides, and how it is managed.

The proposed sub-categories are justified as follows:

(a) Criticality – this focuses on the criticality of the device in terms of impact on the overall operational process and how easy it is to repair or replace a faulty or malfunctioning device. The greater the impact and the more difficult it is to replace or repair, the greater the security risks arising from any attempts to attack or interfere with the device. Safety critical devices clearly need to be engineered and designed to higher standards than those where the is little impact and they are easy to replace.

(b) Function – this class is used to describe the principal function(s) of the device. When considering a device with analytic functions, the nature of the algorithm(s) used is relevant.

(c) Relationships – this class is intended to allow understanding of how the device relates to other devices and the processes, systems or environment within which it operates. For example, a temperature sensor in a room may be linked to an aggregating or control device, as its role is to measure the temperature in the space that it is installed in, it is part of an environmental conditioning process and it will be affected if a door or window is opened or left open in the space within which it is located.

(d) Management interface – relates to how the device is configured, turned on/off or otherwise controlled.

Using this category, the PLC may be described as:

Device → Function → Control

→ Criticality → High

→ Ease of repair → Easy

→ Management interface → Remote

→ Relationships → To other devices → Sensors → Voltage

→ Relationships → To other devices → Actuators → Switch

→ Relationships → To other devices → Control → RTU

4.6. Technology

The proposed technology characteristics of the IIoT device are illustrated in Fig. 7. These focus on technical features that may constrain or influence device design or the ability to address vulnerabilities once the device has been deployed.

The power source, energy use and hardware characteristics are relevant as they can constrain the processing capacity of the device, which in turn affects the design of security mechanisms used to protect the connectivity and may limit the ability to patch or update the device once deployed. The operating system, software type and updatability are relevant given the launch of IoT botnets, for example the Mirai botnet [58,59], as they represent a potential vulnerability and if not updateable may limit the ability to respond to botnet malware. The identity of the device manufacturer and a unique identifier are

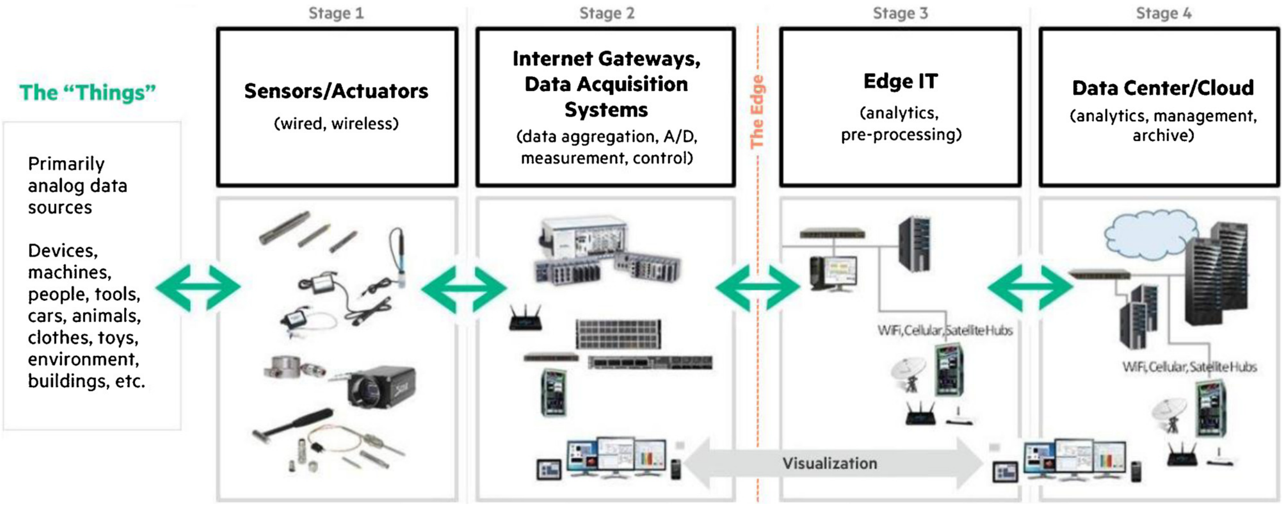
Stage 1
Stage 2
Stage 3
Stage 4
The "Things"
Primarily analog data sources
Devices, machines, people, tools, cars, animals, clothes, toys, environment, buildings, etc.
Sensors/Actuators
(wired, wireless)
Internet Gateways, Data Acquisition Systems
(data aggregation, A/D, measurement, control)
The Edge
Edge IT
(analytics, pre-processing)
Data Center/Cloud
(analytics, management, archive)
WiFi,Cellular,Satellite Hubs
WiFi,Cellular,Satellite Hubs
Visualization

Fig. 3. A 4-Stage IoT solutions architecture© HPE.

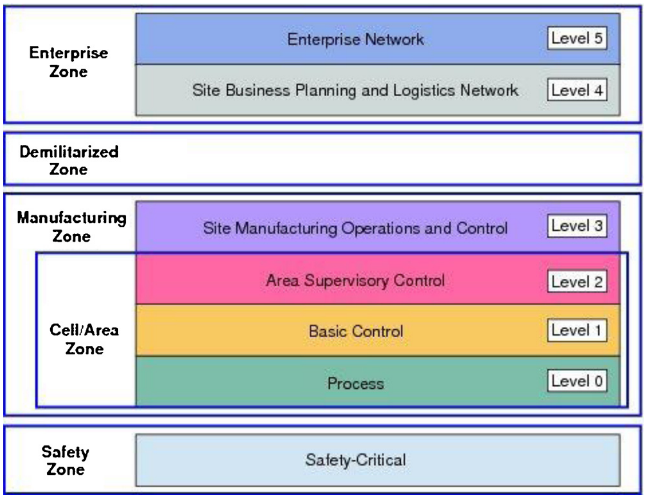

Fig. 4. Purdue Reference Model.

important for configuration management purposes.

Given the nature of IIoT devices and their extensive use of software the concept of trustworthiness is an important technical characteristic. This sub-category references the publicly accessible specification (PAS 754) [60], which provides a framework designed to cover all aspects of the system and software lifecycle, as defined by ISO/IEC 15288 [61]. Of particular relevance is the trustworthiness level matrix [62], which considers the degree of trustworthiness required from a component, composed sub-system or system is dependent on software and the potential impact. Thus, for a component where software provides the sole source of trustworthiness if the impact is deemed significant or critical a high level of trustworthiness should be required and demonstrated.

Using this category, by way of example, an Arduino-based PLC [63] can be described as:

Technology → Power source → Hardwired → Mains
→ Energy use → Always on
→ Operating system → Software & hardware → Arduino
→ Software type → Open source
→ Software updates → Update method → Manual
→ Hardware → CPU type → ATmega2560
→ Hardware → CPU speed → 16 MIPS
→ Hardware → Memory size → 8,192 Bytes
→ Hardware → Storage capacity → 4096 Bytes
→ Manufacturer → CONELCOM GmbH

4.7. User

The proposed user characteristics, as illustrated in Fig. 8, are intended to allow identification of who or what the device is interacting with. The proposed user types are either a human or machine, for example where the device is sensing and providing machine-to-machine communication for system control or monitoring purposes. With regards to the user interface, a device may be:

(a) headless, i.e. there is no indication of device status, measurements or operation;
(b) direct, either passive (e.g. a room thermostat displaying temperature but not allowing user control) or active (e.g. a device with an interactive touch-sensitive display that allows interrogation of the device status and may permit some control of it);
(c) indirect, i.e. the device can be interrogated via another device in the IIoT system.

Using this category, the PLC may be described as:

User → User type → Machine
→ User interface → Indirect → Active

5. Discussion, gaps and recommendations for future research

The approach used to develop our analysis framework is consistent with that used by MITRE in the development of their MAEC [64] method used for malware attribute enumeration and characterisation. As with the development of MAEC, it is inappropriate to employ a taxonomy based on a single top-down tree structure as specific instances or applications of an IIoT device may result in its classification under multiple branches of the tree. The value of our proposed multi-dimensional approach is that it allows classification of an IIoT device based on pre-defines attributes that can be used in systematic studies. Depending on the nature of a study, the researcher can decide which categories and classes to employ, thus allowing the focus to be narrowed or broadened to suit the specific research question. For example, if the focus of a study was on software vulnerabilities, the researcher could choose to ignore industry sector and user type, and focus on the following categories:

- device location and connectivity – to allow assessment of the degree of exposure of the device to potential attacks;
- device characteristics and technology – enabling assessment of the nature and criticality of the software, ease of software updates and systematic risks associated with the processing platform and operating system in use.

The framework set out in this paper provides a mechanism for systematic collection of information about IIoT devices. It was developed as part of a research initiative investigating IIoT security issues. The data collection and analysis is ongoing, however the development of this framework potentially allows comparison of threats and vulnerabilities between different sectors ad application in much the same way as the MAEC approach discussed above.

Having presented our analysis framework, during our research several observations were made which the authors believe to constitute gaps that could be addressed by further research. These recommendations are not presented in any order of importance; we note that each is critical to ensuring future understanding, resiliency and security within IIoT ecosystem, and therefore make no judgement as to their relative importance.

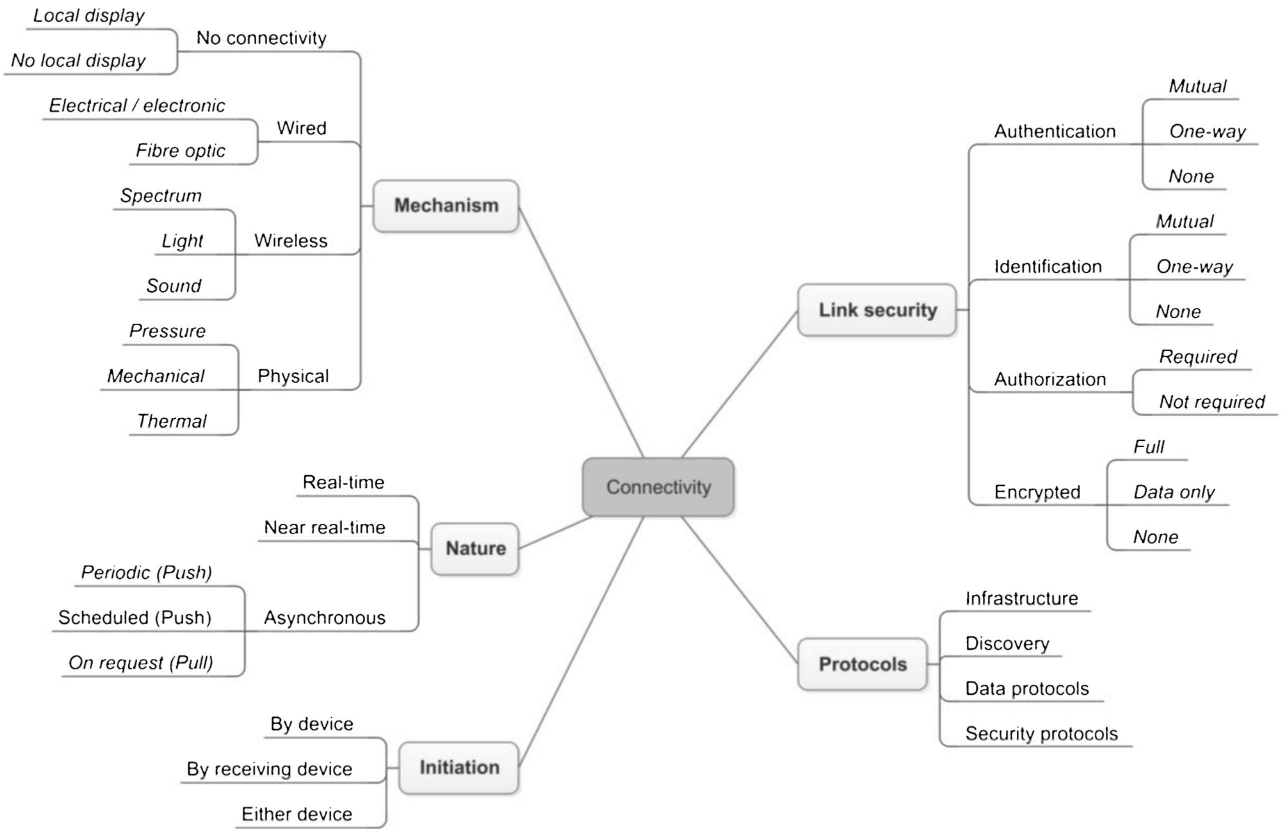

Fig. 5. Connectivity category.

5.1. *Mapping the IIoT ecosystem and threat landscape*

There are a number of publications available that explore and analyse issues of security and privacy relating to IoT in general, there is little work specifically focusing on the IIoT ecosystem. We propose using our taxonomy, to explore and better understand the IIoT ecosystem and associated threat landscape, so as to identify vulnerabilities and potential security and/or privacy concerns.

5.2. *Limited research on OT and ICT convergence*

Whilst there is some work, primarily analyst [65] or vendor [66], driven, which directly states or implies that IIoT is the result of convergence between Operational Technology (OT) and traditional information and communication technologies (ICT). For example, it is suggested [67] that:

> '… merging IT and OT isn't an easy task. Merging these two areas requires well-defined, scalable standards that span from assets to data centers and vice-versa. It's also crucial that these standards are secure, otherwise critical and expensive operational assets can be vulnerable. All these concerns can be tackled by following the concept of 'Enterprise Architecture'.'

The above approach is indicative of a lack of understanding of the differences between conventional enterprise ICT systems and the cyber-physical systems that are found in industrial applications. In contrast, a better-informed assessment [68] of the security challenges faced in securing IoT devices recognised some of the constraints:

> "These current security mechanisms, based on 'traditional public-key infrastructures will almost certainly not scale to accommodate the IoT's amalgam of contexts and devices.'

In this assessment, the authors were taking into account the limitations of IIoT devices, for example, sensors, actuators and RFID tags, where there are processing, power and economic constraints limiting the use of strong encryption.

In addition to these technical issues, there is also the mismatch between the relative short lifespan of many ICT devices and the relative longevity of IACS devices, which are often expected to have a lifespan an order of magnitude longer than their ICT counterparts. We propose to use our analysis framework as a basis for exploring the IT/OT convergence issues.

5.3. *Providing solutions to brownfield issues*

Legacy systems, i.e. a brownfield site, inject complexity into a wide range of cases. A compelling argument has been made [69] regarding the need for developers to considering the issue of brownfield IIoT:

> …how important in industrial IoT (IIoT), such as smart buildings, bridges, roads, railways and all infrastructure that have been around for decades and will continue to be around for decades more.

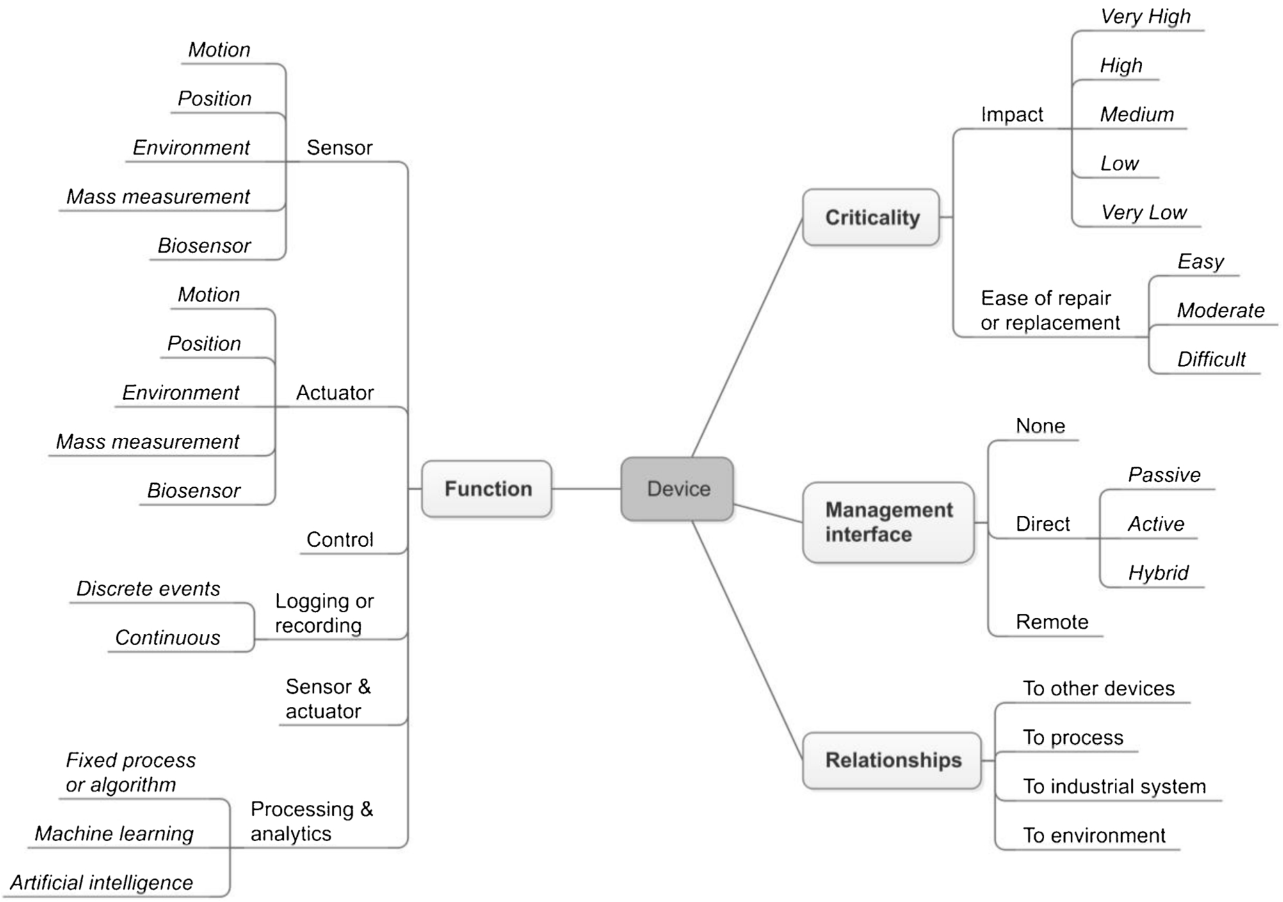

Fig. 6. Device category.

Further research is required to consider the implications of installing IIoT devices in an operational architecture, where security has been implemented using the zones and conduits inherent in the Purdue Model. As with the topics of security and scalability of IIoT, circular conversations are occurring, solutions are required that address both greenfield and brownfield installations, and again the relative longevity of IACS device needs to be taken into account.

5.4. Limited research on safety and security of IIoT devices

Safety and security should be paramount in industrial systems to prevent harm and minimise threat to personnel, assets and the environment. There is increasing industry recognition that safety and security are related [70], for example that connectivity brings both opportunity and risk and that poor security threatens safety. This is also recognised in international functional safety standards [71,72]. With traditional IACS systems, the application of the security principles in based on international standards [73], which advocate use of security models aimed at delivering defence in depth, particularly with reference to connections between different layers in the Purdue Model and segregation of processes.

The adoption of IIoT undermines these established practices by creating new connectivity from systems to enterprise or cloud-based systems, thus increasing the potential for safety and security related breaches. There is a current lack of consistent approaches to the combined assessment of safety and security risks inherent in deployment of IIoT solutions. A combined framework has been proposed [74], but further work is required to codify its use and test its applicability in industrial plants.

6. Conclusion

In conclusion, having laid out the background including an overview of related terms in section two, we provided a survey of existing definitions of IIoT in section three and developed our own definition which we hope improves on those. In section four we then provided an analysis framework for IIoT devices which provides a practical classification schema for those with an interest in security-related issues surrounding IIoT. The use of the schema has been illustrated by examples at the end of each of the sections describing the six categories. Finally, in section five, some gaps in the IIoT related literature were identified, which we propose should be addressed as part of our continuing research.

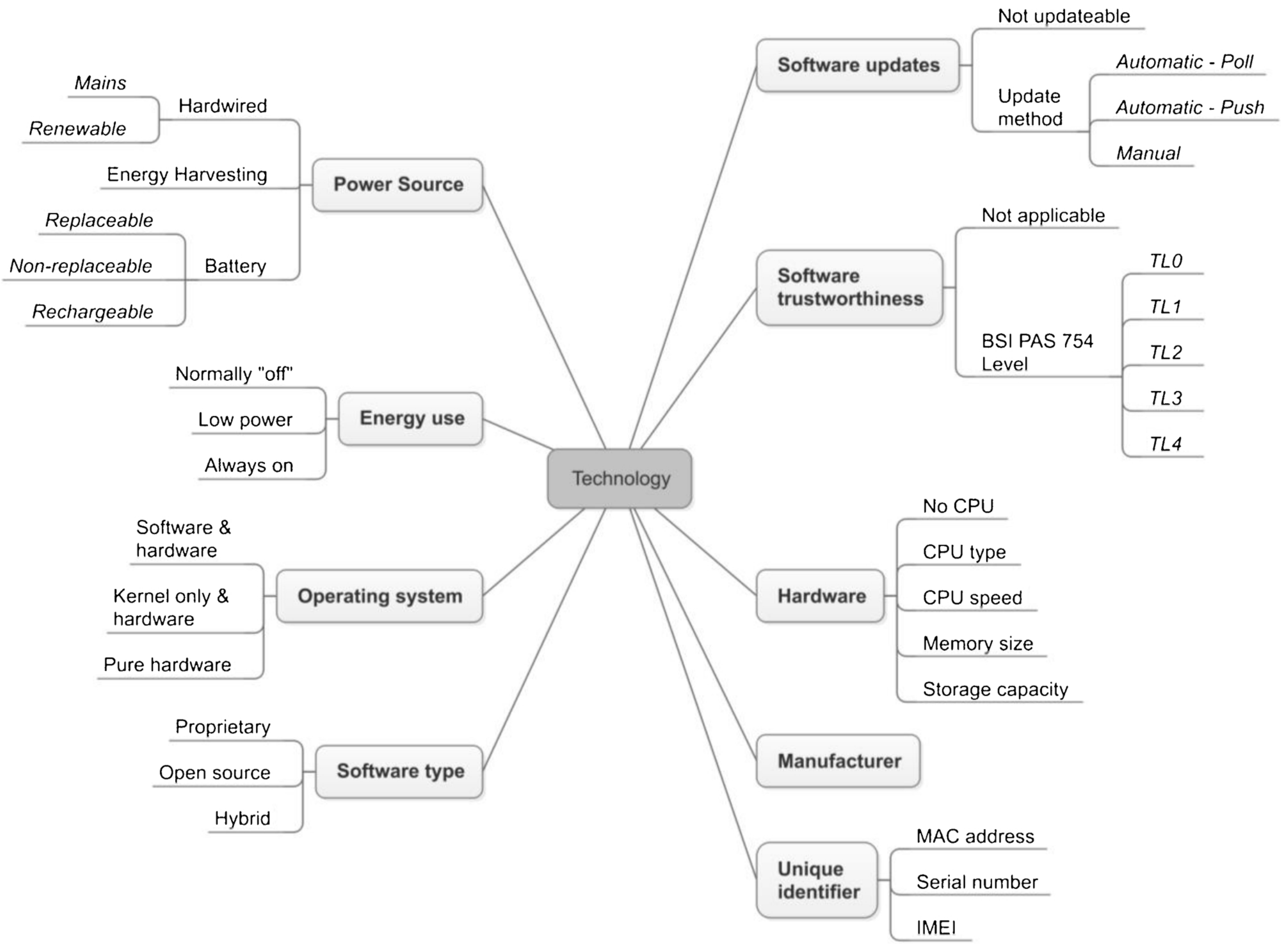

Fig. 7. Technology category.

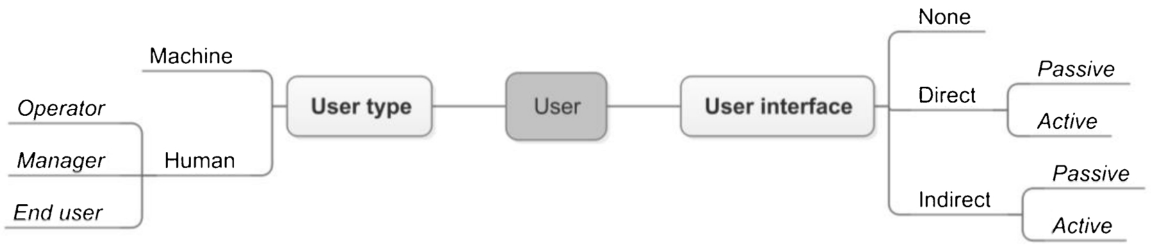

Fig. 8. User category.

Acknowledgements

This work was supported by Cyber Security of the Internet of Things [UK EPSRC Grant EP/N02298X/1].

References

[1] K. Rose, S. Eldridge, L. Chapin, The internet of things: an overview, Internet Soc. (2015) 7.
[2] Beecham Research, M2 M Sector Map, (2014) Available: http://www.beechamresearch.com/download.aspx?id=18.
[3] D. Lukač, 'The fourth ICT-based industrial revolution', 23rd Telecommunications Forum Telfor, IEEE, 2015, pp. 835–838.
[4] Industrie 4.0 Available: vailable: https://www.bmbf.de/de/zukunftsprojekt-industrie-4-0-848.html.
[5] Industrial Internet Consortium, What Is the Industrial Internet? [online], (2018) Available: https://www.iiconsortium.org/about-industrial-internet.ht.
[6] M. Hermann, T. Pentek, B. Otto, Design Principles for Industrie 4.0 Scenarios: A Literature Review, Technische Universität Dotmund, 2015, p. 11 Working paper (Accessed 12 September 2017).
[7] NIST, Framework for Cyber-Physical Systems. Release 1.0, NIST Cyber Physical Systems Public Working Group, (2016), p. 1. Available: http://www.nist.gov/.
[8] CHESS, Chess – Center for Hybrid and Embedded Software Systems. [ONLINE], (2017) Available at: http://chess.eecs.berkeley.edu/.
[9] R. Baheti, H. Gill, Cyber-physical systems, in: T. Samad, A.M. Annaswamy (Eds.), The Impact of Control Technology, vol. 2, IEEE Control Systems Society, New York, 2011, pp. 161–166. Available: http://ieeecss.org/main/IoCT-report.
[10] R. Poovendran, Cyber–physical systems: close encounters between two parallel worlds [point of view], Proc. IEEE 98 (8) (2010) 1363–1366.
[11] Q. Shafi, Cyber Physical Systems Security: A Brief Survey. In Computational Science and Its Applications (ICCSA), 2012, 12th International Conference on (pp. 146–150). IEEE, 2012.
[12] H. Boyes, A security framework for cyber-physical systems, WMG CSC Working Paper, Coventry, University of Warwick, 2017.
[13] K. Stouffer, et al., Guide to Industrial Control Systems (ICS) Security, (2015), p. 1, http://dx.doi.org/10.6028/NIST.SP.800–82r2 NIST special publication, 800(82)r2.
[14] ENISA, ICS SCADA. [online], (2017) Available: https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/scada.
[15] S.A. Boyer, SCADA: Supervisory Control and Data Acquisition, Instrument Society of America, Research Triangle Park, North Carolina, 1993 ISBN 1-55617-210-9. p.9.
[16] J. Falco, et al., IT Security for Industrial Control Systems, (2015) Available at: http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=821684 . (Accessed 4 October 2017) Appendix I.
[17] ibid.

[18] Dpstele. com, What Is SCADA? Real-world Remote Monitoring Elements and Applications. [online], (2017) Available at: http://www.dpstele.com/scada/what-is.php (Accessed September 6 2017).

[19] P. Eden, et al., SCADA system forensic analysis within IIoT, in: L. Thames, D. Schaefer (Eds.), Cybersecurity for Industry 4.0, Springer International Publishing, 2017, pp. 73–101, , http://dx.doi.org/10.1007/978-3-319-50660-9_4.

[20] M. Fahrion, Evolving from SCADA to IoT. Remote Monitoring and Control Conference. [online], (2014) Available: http://www.remotemagazine.com/conferences/wp-content/uploads/2014/11/BB-Electronics.pdf.

[21] J. Leber, General Electric's San Ramon Software Center Takes Shape MIT Technology Review [online], (2012) Available: http://www.technologyreview.com/news/507831/general-electric-pitches-an-industrial-internet/ (Accessed September 8 2017).

[22] D. Floyer, Defining and Sizing the Industrial Internet, Wikibon, June 27, 2013 [online], (2013) Available: http://wikibon.org/wiki/v/Defining_and_Sizing_the_Industrial_Internet.

[23] ge.com, Industrial Internet Insights Report for 2015. [online], (2015) Available at: https://www.ge.com/digital/sites/default/files/industrial-internet-insights-report.pdf (Accessed September 8 2017).

[24] B. Dorsemaine, et al., Internet of things: a definition and taxonomy, Proc. – NGMAST 2015 9th Int. Conf. Next Gener. Mob. Appl. Serv. Technol. 2016 (2015) 72–77, http://dx.doi.org/10.1109/NGMAST.2015.71.

[25] K. Rose, S. Eldridge, L. Chapin, The internet of things: an overview, Internet Soc. (2015) 12.

[26] P. Satyavolu, et al., Designing for Manufacturing's 'Internet of Things'. Cognizant Report. p.4 [online], (2014) Available: https://www.cognizant.com/InsightsWhitepapers/Designing-for-Manufacturings-Internet-of-Things.pdf.

[27] L. Aberle, A Comprehensive Guide to Enterprise IoT Project Success, IoT Agenda, 2015, p. 1. Available: http://internetofthingsagenda.techtarget.com/essentialguide/A-comprehensive-guide-to-enterprise-IoT-project-success (Accessed 10 September 2017).

[28] World Economic Forum, Industrial Internet of Things: Unleashing the Potential of Connected Products and Services, World Economic Forum Industry Agenda, 2015 (available at: http://www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf (Accessed 11 October 2017).

[29] J. Conway, The Industrial Internet of Things: An Evolution to a Smart Manufacturing Enterprise, Schneider Electric Whitepaper, 2015, p. 2.

[30] P. Helmiö, Open Source in Industrial Internet of Things: A Systematic Literature Review Master's Thesis, School of Business and Management, Lappeenranta University of Technology, 2018, p. 21.

[31] Real Time Innovations Inc, Industrial Internet of Things, RTI FAQ, 2015, p. 1 (Available: https://info.rti.com/hubfs/docs/Industrial_IoT_FAQ.pdf . (Accessed 29/September 2017).

[32] D. Spath, et al., Produktionsarbeit zer Zukunft –Industrie 4.0, Fraunhofer Verlag, Stuttgart, 2013.

[33] V. Emmrich, et al., Geschäftsmodell-Innovation durch Industrie 4.0: Chancen und Risiken für den Maschinen- und Anlagenbau, Dr. Wieselhuber & Partner, and Fraunhofer IPA, Munich and Stuttgart, 2015.

[34] T. Kaufmann, Geschäftsmodelle in Industrie 4.0 und dem Internet der Dinge, Der Weg vom Anspruch in die Wirklichkeit (Essentials), Springer Vieweg, Wiesbaden, 2015.

[35] B. Dorsemaine, J.P. Gaulier, J.P. Wary, N. Kheir, P. Urien, Internet of things: a definition and taxonomy, Proc. – NGMAST 2015 9th Int. Conf. Next Gener. Mob. Appl. Serv. Technol. (2016) 72–77, http://dx.doi.org/10.1109/NGMAST.2015.71.

[36] L. Püschel, M. Roeglinger, H. Schlott, What's in a smart thing? Development of a multi-layer taxonomy, in: P. Ågerfalk, N. Levina, S.S. Kien (Eds.), Proceedings of the International Conference on Information Systems – Digital Innovation at the Crossroads, ICIS 2016, 2016 Association for Information Systems, Dublin, Ireland, 2016December 11–14, 2016.

[37] CISCO Systems, Converged Plantwide Ethernet (CPwE) Design and Implementation Guide, (2013) Available: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/CPwE_DIG.html . (Accessed 5 October 2017).

[38] V. Rozsa, et al., An Application Domain-Based Taxonomy for IoT Sensors, In ISPE TE, 2016, pp. 249–258.

[39] E. Ahmed, et al., Internet-of-things-based smart environments: state of the art, taxonomy, and open research challenges, IEEE Wireless Commun. 23 (5) (2016) 10–16.

[40] I. Yaqoob, et al., Internet of things architecture: recent advances, taxonomy, requirements, and open challenges, IEEE Wireless Commun. 24 (3) (2017) 10–16.

[41] S. Schneider, The industrial internet of things (IIoT), in: H. Geng (Ed.), Internet of Things and Data Analytics Handbook, John Wiley & Sons, Inc., Hoboken, NJ, USA, 2017, , http://dx.doi.org/10.1002/9781119173601.ch3.

[42] Beecham Research, M2 M Sector Map, (2014) Available: http://www.beechamresearch.com/download.aspx?id = 18.

[43] S. Jeschke, C. Brecher, T. Meisen, D. Özdemir, T. Eschert, Industrial internet of things and cyber manufacturing systems, Industrial Internet of Things, Springer, Cham, 2017, 2018, pp. 3–19, http://dx.doi.org/10.1007/978-3-319-42559-7_1.

[44] CyPhERS, Characteristics, Capabilities, Potential Applications of Cyber-physical Systems: a Preliminary Analysis, (2013) http://www.cyphers.eu/sites/default/files/D2.1.pdf . (Accessed 18 March 2018).

[45] Beecham Research, M2 M Sector Map, (2014) Available: http://www.beechamresearch.com/download.aspx?id = 18.

[46] Department for Business, Energy & Industrial Strategy, Made Smarter Review, (2017) Fig. 16. p51. Available: https://www.gov.uk/government/publications/made-smarter-review.

[47] M.E. Porter, J.E. Heppelmann, How smart, connected products are transforming competition: spotlight on managing the internet of things, Harv. Bus. Rev. 92 (11) (2014) 64–88.

[48] E. Fleisch, M. Weinberger, F. Wortmann, Geschäftsmodelle im internet der dinge, Schmalenbachs Zeitschrift für betriebswirtschaftliche Forschung 67 (4) (2015) 444–465.

[49] L. Püschel, M. Roeglinger, H. Schlott, What's in a smart thing? Development of a multi-layer taxonomy, in: P. Ågerfalk, N. Levina, S.S. Kien (Eds.), Proceedings of the International Conference on Information Systems – Digital Innovation at the Crossroads, ICIS 2016, vol. 2016, Association for Information Systems, Dublin, Ireland, 2016December 11–14, 2016.

[50] OWASP, IoT Framework Assessment, in Internet of Things (IoT) Project, (2018) Available: https://www.owasp.org/index.php/IoT_Framework_Assessment.

[51] T. Bradicich, The Intelligent Edge: What It Is, What It's Not, and Why It's Useful, Hewlett Packard Enterprise, (2017) Available: https://www.hpe.com/us/en/insights/articles/the-intelligent-edge-what-it-is-what-its-not-and-why-its-useful-1704.html.

[52] T.J. Williams, The Purdue Enterprise Reference Architecture, International Society of Automation, Research Triangle Park, North Carolina, 1992 ISBN 1-55617-265-6.

[53] T.J. Williams, The Purdue enterprise reference architecture, Comput. Ind. 24 (2–3) (1994) 141–158.

[54] ANSI/ISA 99.00. 01-2007, Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models, 2007.

[55] IEC/TS 62443-1-1 ED. 1.0 EN:2009, Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models.

[56] L. Obregon, Secure Architecture for Industrial Control Systems, The SANS Institute, 2014 Available: https://www.sans.org/reading-room/whitepapers/ICS/secure-architecture-industrial-control-systems-36327.

[57] Health, Safety Executive, Cyber Security for Industrial Automation and Control Systems (IACS), (2017) Bootle, Merseyside. Available: http://www.hse.gov.uk/foi/internalops/og/og-0086.pdf.

[58] C. Kolias, G. Kambourakis, A. Stavrou, J. Voas, DDoS in the IoT: mirai and other botnets, Computer 50 (7) (2017) 80–84.

[59] M. Antonakakis, et al., Understanding the Mirai Botnet, (2017) Available: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis.

[60] BSI, PAS 754 Software Trustworthiness –Governance and Management ?Specification, British Standards Institution, London, 2014.

[61] ISO, ISO/IEC/IEE 15288 Systems and Software Engineering –Systems Life Cycle Processes, International Standards Organisation, Geneva, 2015.

[62] BSI, PAS 754 Software Trustworthiness –Governance and Management ?Specification, British Standards Institution, London, 2014, p. 5.

[63] Controllino Maxi Available: http://controllino.biz/controllino/maxi-automation/.

[64] I. Kirillov, et al., Malware Attribute Enumeration and Characterization. MITRE [online], (2015) Available: http://maec.mitre.org.

[65] K. Steenstrup, et al., Predicts 2017: IT and OT convergence will create new challenges and opportunities, Gartner (2016) Available: https://www.gartner.com/doc/3531817.

[66] C. Hertzog, Smart Grid Trends to Watch: ICT Innovations and New Entrants, (2012) Available: https://www.smartgridlibrary.com/tag/ictot-convergence/.

[67] N. Shah, IT and OT Convergence –The Inevitable Evolution of Industry, Iotforall, (2017) Available: https://www.iotforall.com/it-and-ot-convergence/.

[68] R. Roman, P. Najera, J. Lopez, Securing the internet of things, IEEE Comput. 44 (2011) 51–58, http://dx.doi.org/10.1109/MC.2011.291.

[69] B. Dickson, What Is the Difference Between Greenfield and Brownfield IoT Development? (2016) Available: https://bdtechtalks.com/2016/09/22/what-is-the-difference-between-greenfield-and-brownfield-iot-development/.

[70] Rockwell Automation, Safety Through Security. [online], (2016) Available: http://literature.rockwellautomation.com/idc/groups/literature/documents/wp/safety-wp035_-en-p.pdf.

[71] BSI, BS EN 61508-1 Functional Safety of Electrical/electronic/programmable Electronic Safety-related Systems. Part 1: General Requirements, British Standards Institution, London, 2010 Clause 7.4.2.3. p.27.

[72] IEC, IEC 61511-1:2016 Functional Safety – Safety Instrumented Systems for the Process Industry Sector – Part 1: Framework, Definitions, System, Hardware and Application Programming Requirements, International Electrotechnical Commission, Geneva, 2016.

[73] IEC, 62443 – Industrial Communication Networks – Network and System Security. Suite of Standards, International Electrotechnical Commission, Geneva, 2018.

[74] H. Boyes, A security framework for cyber-physical systems, WMG CSC Working Paper, Coventry, University of Warwick, 2017.