Journal of Systemics, Cybernetics and Informatics (2022) 20(2), 51-62
https://doi.org/10.54808/JSCI.20.02.51

Investigating Data Risk Considerations in Emergent Cyber Physical Production Systems

Gerard WARD
Information Systems and Operational Management, Business School, The University of Auckland, Auckland 1010, New Zealand

Lech JANCZEWSKI
Information Systems and Operational Management, Business School, The University of Auckland, Auckland 1010, New Zealand (NZ)

ABSTRACT [1]

The Industrial Internet of Things (IIoT) describes a computing model where ubiquitous networks of heterogenous devices equipped with embedded sensors and actuators support innovative data-centric business models. Emergent IIoT use cases include Cyber Physical Production Systems (CPPS) to support asset optimization through self-organization of modular machines within production systems. In CPPS, raw materials, machines, and operations are interconnected to form a tightly integrated network.

To ensure manufacturing continuity as CPPS networks evolve, asset managers will need to evaluate risk across multi-disciplinary domains. The domains have different architectures, lexicons, and priorities. To contribute to the eventual codification of data risk in CPPS, this research builds on previous literature to consider how data may traverse the CPPS model. The resulting models put forward in this research are informed by a transdisciplinary panel of experts drawn from disciplines including information and operational technology to bring greater specificity to the definition of business-critical data in supporting IIoT. Based on these expert views, a conceptual hierarchical automation architecture that may characterize many future state production processes is presented.

Keywords: Industrial Internet of Things (IIoT), Cyber Physical Production Systems, Risk Analysis, Security, Operational Technology, Information Technology, Industry 4.0.

[1] Contact author: gerard.ward@auckland.ac.nz
We would like to thank the following peer-review editors. Dr Brian Cusack, Faculty of Engineering, Computer and Mathematical Sciences, Auckland University of Technology, NZ. Dr Bryce Antony, Senior Cyber Security Engineer, AdvantageNZ, Palmerston North, NZ. Mr Koro Tawa, Professional Teaching Fellow, Information Systems and Operations Management, the University of Auckland, NZ.

1. INTRODUCTION

Within IIoT, Cyber Physical Systems (CPS) refers to systems that integrate the computation and networking necessary to control physical processes bound by feedback loops [1]. For industrial manufacturing, Cyber Physical Production Systems (CPPS) describes a conceptual environment in which the attributes of CPS are extended to include the "5Cs: connection, conversion, cyber, cognition, and configuration" [2].

Supporting these 5Cs in CPPS is the learned state necessary to provide for "adaptive, self-configuring and partly self-organizing, flexible production plants" [3]. Achieving this necessitates the data-centric model relying on continual data analysis to uncover previously unknown cause-and-effect relationships [4]. Therefore, CPPS will likely compose modules or components, which together fulfil a certain function, or can be reconfigured to achieve another function. These module referred to as Cyber Physical Production Modules (CPPM) will consist of heterogenous components [3] bound by *Things* connected to the Internet [5].

It is these *Things* in the Internet-of-Things (IoT) that sense conditions [5], with that sensed data carried over the Internet to connect with other sensor nodes, which support collaboration. Extending the IoT, CPS-embedded devices complement the IIoT by increasing "knowledge about the physical system of interest" [6]. Supporting this continual analysis of data in the IIoT are computationally powerful smart actuator and sensor devices connected to Mist, Fog and the Cloud, which use virtualization technologies. Cloud refers to Internet-hosted data, and Fog refers to distributed computing, where computation is completed midway between the sensors and actuators to minimize data traffic and network latency. Mist refers to lightweight fog computation placed closer to the Things. Virtualization refers to the division of physical servers into multiple virtual server instances. This pooling of computing power supports optimization. However, the software-defined abstraction of the underlying hardware still presents security issues. It is considered that the use of

Cloud, Fog, and Mist technologies will bring flexibility to the hierarchies that characterize manufacturing automation [7]. Assisting flexibility are Software Defined Networks (SDN), a recent network paradigm that virtualizes physically distributed network hardware in software [8]. In SDN, the centralised software backplane supports scalability and improves security through process isolation, micro segmentation [9], and Zero-Trust [10]. Additionally, many CPPM applications may use containerized microservices, an increasingly popular software architecture that can be readily modified and deployed. While loosely coupled, which reduces the risk in interdependencies across the system, microservices have a reliance on widely distributed communication interfaces [11].

Based on these technologies, CPS focuses on the integration of computation, networking and physical processes at a micro method level. In contrast, IIoT supports the macro functions through the transformation of information flowing from "machines, CPSs, advanced analytics, AI [Artificial Intelligence], people, cloud, and edge computing" in a connected, integrated manner [2]. In this research AI refers to software-defined and data-centric algorithms.

The continuing trend in integration of Information Technology (IT) and Operational Technology (OT) has been conceptualized as Industry 4.0 (also Industrie 4.0 or I4.0). I4.0 is described as a data-centric paradigm characterized by an "ability to accelerate corporate decision-making and adaptation processes" informed by "interconnectedness between cyber-physical systems and people" [4]. The concept of I4.0 emerged from academia and the German government, and the term IIoT was coined by General Electric to describe Internet-enabled Machine to Machine (M2M) communication. This research uses the term IIoT, as the objectives of I4.0 align with those of the IIoT.

Challenging precision in defining CPPS within IIoT is that its use-cases are a "thematic subject as opposed to a disciplinary topic" [12]. While emerging from IT and electrical engineering, [12] postulates that multi-disciplinary fields such as CPPS often start as themes before becoming codified. For example, in considering Artificial Intelligence (AI) in IIoT, the International Organization for Standardization (ISO), a Standards Developing Organization (SDO), currently lists 32 standards specific to AI. Of these 32 standards, 9 (28%) are published and 23 (72%) are under development [13]. Those under development include the use of AI in standards such as *Functional safety and AI systems, as well as Risk Management* [13], which are relevant to the IIoT. Adding complexity to identifying the issues and risks specific to IIoT implementations is the fact that different technical specialties have their own lexicons and differing rates of system change. Moreover, the International Electrotechnical Commission (IEC) considers that a challenge to IIoT adoption is the lack of technical standardization [2].

Illustrating emergent IIoT type use-cases, Congnizant [14], a US-based technology company, states that use of IoT data to deliver tighter integration between a pharmaceutical client's manufacturing and ERP systems delivered a 20% increase in production output. Also, a US tool manufacturer's digital transformation, which focused on the use of IoT-derived data, has led to operational improvements projected to deliver US$100 million in cost savings over 5 years [14]. Nonetheless, these use-cases are not exact CPPS implementations, so extending the functionality implicit in these case-studies into more complex self-organizing paradigms will require robust risk management.

To contribute to the process of CPPS risk evaluation, given these challenges, this research presents generalized process boundaries showing the critical data interchange that will help asset owners to consider the priorities that risk identification must account for. To achieve this the expert input of a transdisciplinary panel of IT, OT, AI, and Legal and Risk experts informed the refinement of the conceptual model alongside key risk considerations.

To satisfy the objective of this research around contributing to the development of a systems approach to risk assessment in CPPS, this paper is structured as follows. Section 2 discusses the evolution of Industrial Automation and Control Systems (IACS) and key data considerations, including the current state of standardization. Section 3 sets out the methodology adapted for use in this research. Section 4 brings specificity to where CPPS sits within the IIoT paradigm. Section 5 addresses how traditional data hierarchies will be compressed as an increased fidelity of business-critical data is supported by new technologies. Section 6 sets out the model validation methods used. Section 7 presents the findings in a taxonomy. Section 8 explains this research's future direction, with Section 9 acknowledging the experts and reviewers who have kindly contributed to this research program.

2. FOUNDATIONAL TECHNOLOGIES

Related Work

Across IT systems the CIA Triad (CIA) is used to broadly approximate the essential data properties of Confidentiality, Integrity, and Availability [1]. For OT, CIA is situationally modified to include data Availability and Integrity, given that they are key to process correctness, followed by Confidentiality (AIC) [1]. In OT safety-critical processes, Safety is added as SAIC, to emphasize the process redundancy necessary to ensure the data integrity required of functional safety systems. Process integrity is vital, as failures could result in injury or death, environmental degradation, and/ or significant

economic disruption. Criticality means different things across the different domains in the IIoT, so key considerations are discussed in the following sections.

Industrial Automation and Control Systems (IACS)
For processes in CPPS that are critical, the system will draw on IACS, a class of industrial computing within the domain of OT. IACS comprises hardware, data networks, and software.

The progressive refinement of standards that provide a baseline of functional attributes has assisted the reduction of risk in the operation of IACS. Examples include: *IEC 62443 - Industrial Automation and Control Systems (IACS)*; IEC 61508 covering functional safety of programmable electronic safety systems; and for data security in networks and systems, the IEC 62243 series. When in control of hazardous processes, IACS will include the layering of redundant systems necessary to ensure the level of process safety specified in IEC 61508.

In IACS systems, risk is defined as "a function of the frequency of an unwanted dangerous event and the severity of the consequences of that event/hazard" [15]. Illustrating the differing lexicons across IT and IACS, the IT standard ISO 27001 (part of the 27000 IT security series) includes a single reference to hazard. It refers to environmental hazards that threaten IT equipment [16], but not to equipment preventing the IACS categories of hazard that risk injury or the loss of life. Contributing to these different lexicons is that IT and OT are discrete disciplines characterized by differences including:

- *Separate architectures*: the two domains have different computational priorities in that OT emphasizes process correctness, whereas IT emphasizes performance.
- *Communication protocols*: conflicting protocols may cause OT systems to enter an unsafe state [17].
- *Asset lifespan*: the IT asset lifecycle is typically 3 to 5 years, whereas IACS assets may be required to last for 30 years or more [18].
- *Divergent design*: safety is a critical OT design criterion [17], whereas IT prioritizes confidentiality and integrity.
- *Hardware versus software*: traditionally IT has utilized software security protections, and OT has favored hardware [17].

To provide for process continuity, risk management is the discipline that, following the identification of issues and appropriate compensating controls, reduces the risk of vulnerabilities being exploited to organizationally acceptable levels. With regard to data, the level of control applied needs to be proportionate to the process or function that the data supports; i.e., the economic value derived from that data in supporting the fidelity of organizational decision making.

Verification and Validation (V&V)
To assist the identification of vulnerabilities that could threaten SAIC, Verification and Validation (V&V) is used to measure how well the behavior of a physical system matches that of the engineering model it approximates [19]. Validation examines the processes used to determine that the right system was built, and the resulting behavior of the physical system [20]. Verification is used to ensure the system meets its functional requirements, including safety [20]. V&V is critical to the quality management necessary to ensure system integrity. Risk management is then used to further reduce the inherent risk to be within organizationally acceptable tolerances. Alongside V&V, certification is the quality management process where the robustness of V&V is assessed, often by an independent third party.

Safety-Critical Data
Reflecting the need for sequence in the way things happen, in support of OT correctness, the requirement for real-time execution gives rise to fundamental differences between IT and OT architectures. OT requires that processing tasks have set priorities, such that no lower-value task can execute before higher-value critical tasks [21]. In contrast, IT processing uses speculative execution, whereby instruction sets are loaded into memory in anticipation of their being called. Speculation lacks the precision required of OT critical task sequencing, and therefore process correctness [21].

Where hazards are present, and subject to the damage that could result from failure, Safety Instrumented Systems (SIS) are implemented to support fail-safe conditions [22]. SIS describes the hardened hardware and software that are implemented to ensure functional safety is maintained when abnormal operating conditions are encountered. In safety-critical systems, Defense in Depth (DiD) is considered during the design stage, with multiple levels of redundancy included to reduce the risk of serious accidents to be within an acceptable range [23]. DiD also addresses the risk that "a safe failure of one function may create a new hazard or be an additional cause for an existing hazard" [16].

Illustrating the risks to SIS, in 2017, nation state actors compromised an SIS installed in a Saudi Arabian oil refinery [24]. While the SIS had accidently been left in an incorrect operating state, researchers postulate it was only an error in the code of the TRISIS malware that prevented it from being capable of triggering a refinery explosion [25]. It is considered that TRISIS was likely installed following a compromise of the intermediatory IT networks used for remote access to the IACS [25]. So while attacks against OT assets are increasing, typically IT assets are used as the intermediary attack vector [1].

Business-Critical Data

Differentiating safety-critical from business-critical data is the fact that the OT term 'safety' addresses control of physical processes. These are processes for which failures are kinetic, and thus could cause physical damage. The consequences of failures in securing business data are typically financial or reputational [1]. Reputational losses may include loss of market share. Therefore, the risk controls appropriate to business-critical data are those associated with IT systems, so they approximate CIA.

Illustrating business-critical issues, in May 2021 a ransomware attack of IT systems resulted in the five-day shutdown of a key US pipeline. This economically critical asset supplies 45% of the fuel consumed on the US's east coast [26]. While Colonial Pipeline's IT systems served as the attack vector, the co-dependency of the IACS systems on the billing systems installed in the IT domain meant customers could not be charged for usage. As this business-critical information was unavailable, this contributed to Colonial's IACS systems being shut down. Therefore, where vulnerabilities are present in the legacy cores of IT, given the tight integration across domains that IIoT presents, new classes of operational risk may arise from these tightly integrated co-dependencies.

Like OT, IT also embraces the concept of DiD. In IT, DiD refers to successive layers of countermeasures necessary to thwart a threat actor pursuing the same attack vector [27]. Therefore, in IT deployments, DiD is a threat isolation mechanism protecting the interior from exterior disturbance. Highlighting different priorities, for IACS, DiD is a hazard containment mechanism, protecting the outside from internal process disturbance. For IT, DiD is dynamic, in that additional countermeasures may be introduced over time, or upgraded at frequent intervals. For IACS, the asset life, and the need to support continuous and potentially hazardous processes, limits the opportunity for new technologies to be introduced. Changes to IACS systems will necessitate further V&V, whereas changes to IT systems typically do not.

IoT and IIoT Protocols

A characteristic of IIoT environments is the integration of protocols, standards, and data buses of different technologies [28] necessary to support device and machine interoperability. While IT typically relies on the dominant and standardized TCP/IP protocol (or the IP variant, UDP), a multiplicity of communication protocols support differing IIoT use-cases.

Those protocols targeting IoT and IIoT typically have trade-offs relative to performance, security, and energy consumption. For example, Lora is an open-standard, low-power physical layer protocol. Supporting the cyber layer, LoraWan extends connectivity across wide area networks up to 20km in range bidirectionally, and is normally deployed in a single-hop star network topology [29]. LoraWan's security includes each smart device using robust AES data encryption, and globally unique identifiers to support device identity management [29]. However, weaknesses include encryption key management using long-term keys, and encryption functions relying on repetitive cipher patterns [28].

Illustrating threats, in late 2021 a key US cyber agency, CISA [30], released an alert advisory that an open source middleware protocol, Data Distribution Service (DDS), which is used to integrate business-critical IoT systems, could be exploited. Exploitation risks include Distributed Denial of Service (DDoS), remote code execution, and information exposure [30]. This middleware has been implemented by NASA, Siemens, and Volkswagen [31].

Standardization of Other Core Technologies

As set out in the previous section, with 72% of AI-related standards currently under development [13], this may challenge the V&V of systems, given the absence of uniform standards, particularly since developing standards is a time-consuming process for SDOs. For example, standardizing 5G specifications spanned 5 years (2015 through 2020) [32]. It is postulated that the rate of research and innovation is now at such a level that traditional SDO processes "will not be able to keep up, speed-wise" [7] [32].

To illustrate the complexity the IIoT presents to risk managers, in investigating the state of 24 standards which may be relevant to a generalised IIoT implementation, [33] identified that of the eight relevant to autonomous determinism in IIoT, four were under development. And within these drafts, while CPPS is referenced, there is no specificity [2]. Moreover the two standards covering *Cyber Physical Production Systems*, which form part of the ISO 23704 series addressing *Cyber-Physically controlled Smart Machine Tools*, are yet to be ratified [34].

Therefore, a generalised risk model that can assist the process of identifying IIoT data risk, as well as emergent CPPS risk considerations, will significantly benefit asset owners as well as researchers. The next section sets out how the model this research presents was refined using expert input.

3. METHODOLOGY

To bring structure to the enumeration of risk across the IIoT ensemble, a pragmatic epistemology is used to map a generalized set of risk attributes across the IIoT technical cores. Alongside the literature cited in this research, the IACS, CPS, and risk considerations discussed have been shaped by the insights of 24

transdisciplinary and heterogenous experts. The experts included 12 with domain expertise across IT, IACS, and IoT. In addition, 12 panellists were experts in AI as well as Legal & Risk. Using the Delphi research method, expert opinion was sought covering risk attributes in the IIoT integration cores relevant to each of the four cohort domains (IT, OT, AI, and Legal & Risk). These findings were used to refine the importance of key themes, as well as the model discussed in the following sections of this research. The IIoT and CPPS-related questions were seeded by a detailed survey of literature using semantic reduction and techniques from Corpus Linguistics, bound by the systematic processes prescribed by PRISMA [1].

Delphi is a data-driven research method used in emergent fields for which empirical evidence is limited [35]. The Delphi method uses semi-structured and open questions during interviews, to identify and refine emergent themes. The heterogenous makeup and size of the panel, comprising 24 transdisciplinary participants, aligns with directions in the existing literature, where [35] found that 59% of Delphi panels comprised between 14 and 30 participants. Moreover, [36] noted that the early advocates of Delphi used and recommended a small panel size for emergent fields.

The panellists' experience was extensive, with an average of 23 years of professional practice. The industry exposure of the IT participants spanned operations and security architects, breach response, risk consulting and academia, with an average of 22.9 years of experience. The OT and IoT participants' knowledge spanned industrial cyber security, electrical and mechanical engineering, as well as academia, with experience averaging 19 years. The Legal and Risk experts averaged 23 years spanning technology law and the underwriting of technology risk for the Insurance markets. Noting that AI in this research is defined as software-defined algorithms, the AI cohort's experience averaged 25.8 years.

The combined average of 23 years of professional experience indicates the information power of this panel to assist in the identification of patterns relevant to data risk considerations in emergent CPPS. Information power refers to the research technique in which the "information richness" of the dataset in research that has a broad aim is inductive and exploratory, and the method is to analyze the entirety of the dataset [37]. Research ethics permission was obtained from the researchers' academic institution prior to this research commencing, and participants consented to their contributions being included in this research. First round one-on-one interviews lasted between 45 and 120 minutes.

A specific focus was how the technical factors specific to the three technical cohorts (IT, OT, and AI) could be grouped under higher-order categorizations of Reputation and Trust. The categorisations were seeded from the detailed survey of literature [1]. Framed by the transdisciplinary panellist insights, Section 4 examines the emergent technological cores that are integrated in the IIoT.

4. IIOT INTEGRATION

CPPS within the IIoT Ecosystem

Fig. 1 summarizes the view of the expert panel that while CPS and CPPS are smart "Things", the functionality resulting from the intersection of IT, OT, and AI is more relevant to business-critical data. Limiting application in safety-critical functions is the issue that the system must not be allowed to self-determine whether an unsafe condition is present or is imminent. Rather, the SIS maintains functional safety when abnormal conditions are encountered.

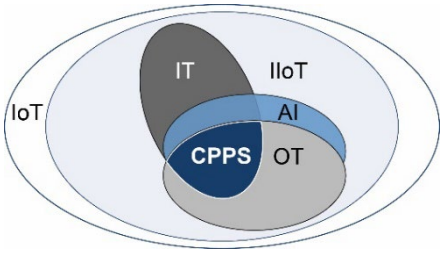

Fig. 1. CPPS, an intersection of technologies.

Supporting CPPS type processing within the estate of IoT as shown in Fig. 1 are smart devices incorporating powerful microcontroller units that may include a central processor, memory, and have Real Time Operation Operating Systems (RTOS) installed. The inbuilt sensors and actuators enable algorithms, often via Internet-enabled communication, to act in concert with Mist, Fog and Cloud to monitor or deterministically control non-critical functions [38]. These functions include performance, threat analysis, and CPPS re-configuration. Given this processing power and Internet-facing connections, onboard and networked threat detection is necessary, as these devices will be subject to IT-type attacks [39]. The literature identifies that device capability in IIoT is characterized by hardware that incorporates unique device identification, measurements (environmental sensors of non-hazardous properties), data transfer, data processing, and actuation to control non-hazardous environmental factors [40].

While CPPS behavior can achieve reliability through the use of error-correction algorithms, relying on a learned state acquired through Machine Learning (ML) [41], verification can be difficult as ML is often viewed as a black box function. Where the OT and AI panel has observed algorithms running on smart devices in support of IACS, they are typically in non-hazardous discrete processes. Furthermore, the ML functions are simpler,

rule-based algorithms used to measure physical change in support of business-critical processes. Nonetheless, increasing computation capacity will be supporting increasing algorithmic complexity, and therefore the dynamism of reconfiguration in CPPS. Algorithms can now compute over a trillion parameters; up from 110 million four years ago [42]. This means the granularity of parameters or connection weights permits programs to"pay attention" to patterns rather than having to work each parameter sequentially [42].

Moreover, the panel view was that the absence of standardization is a constraint on the uptake of these new technologies. For example, elaborating the considerations discussed in Section 2 covering standardization is the fact that AI-related standards such as *Functional safety and AI systems*, and the methodology for *Assessment of the robustness of neural networks*, are under development.

Comparison of CPS and IIOT

To assist the categorization of CPPS and the IIoT, and therefore consideration of risk between them, the differences in the properties and functions flowing from the panel interviews are summarized in Table I.

TABLE I. CPPS AND IIOT ATTRIBUTES

Property	Function	CPPS	Industrial IoT
Data	Protocols	OT or IoT i.e., EtherNet/IP or emergent IoT protocols.	TCP/IP or UDP, and higher layer IoT-adapted protocols.
Model	Business Processes	Micro	Macro
Time	Execution speed	Real time; e.g., milli seconds.	Near real time; e.g., seconds.
Criticality	Functional priority	Safety-critical is not yet standardized. Will rely on IACS.	Business-critical – IT type standardization.
Information	Feedback loops	Low error tolerance (time).	Higher error threshold.
System(s)	Functional capability	Sensing & actuation.	Sensing
Process	Processing objective	Correctness	Performance
Management	Life-cycle Management	Emergent device practices.	IT practices
Control	Functional objective	Physical process	Asset optimization

In Table I, micro describes functions concerned with specific processes (the OT in Fig. 1), whereas macro refers to the entire IIoT ensemble as shown in Fig. 1.

The view of the OT panel cohort is that the goal of adaptive, self-configuring, and self-organizing systems will necessitate change in the hierarchical automation architecture that specifies IACS integration. The next section sets out the challenges posed by the characteristics of CPPS, namely system dynamism and reconfiguration.

5. CPPS DATA MODEL

Standardized Safety-Critical

Fig. 2.A shows a four-layer representation of the ISA-95 Automation Pyramid that generalizes IACS deployments as ratified under the IEC 6226 standard. The Automation Pyramid (pyramid) is applicable to manufacturing processes, whether they are hazardous or not. In Fig. 2.B the pyramid is adapted following panel feedback.

In the traditional pyramid presented in Fig. 2.A, data flow between Level 0 field devices such as sensors and actuators to programmable controllers (PLCs). At Level 1 those data are aggregated by the Supervisory Control and Data Acquisition System (SCADA), which centralizes plant processes. Where the implementation incorporates many devices, these devices may be grouped into semiautonomous subsystems, and networked with a Distributed Control System (DCS).

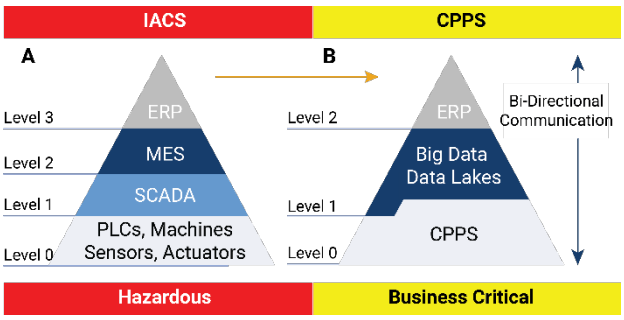

Fig. 2. CPPS compression of the Automation Pyramid.

The DCS supports data collection, analysis, and presentation of control information to human operators [43]. In Fig. 2.A, at Level 2 data are further aggregated in the Manufacturing Execution System (MES), which assists production planning [23]. Data from the MES can also be fed into the Enterprise Resource Planning system (ERP), which integrates the aggregated IACS data with data from other departments to assist enterprise-wide planning.

Based on the panel feedback, Fig. 2.B presents the integration of industrial computing that CPPS supports. Compression of the pyramid is achieved at Level 0, using computationally capable smart devices. The smart devices, including sensors and actuators, control processes at the process source (or at the Fog layer) in concert with other connected smart devices. In Fig. 2.B, the MES is superseded by algorithmic analysis of Big Data (Level 1), which is stored in Cloud data repositories at scale, which are referred to as Data Lakes (DLs) and used to inform business-critical decisions. This can include the retention of temporal process data for use in future ML training to support AI.

While Fig. 2.B illustrates the compression of hierarchies, in this research Fig. 3 extends the decomposition of automation [7] to better account for both safety-critical and business-critical data risk. The panel view was that specificity was necessary to account for the co-dependent risks that CPPS integration models present.

Supporting the decomposition shown in Fig. 2 will be the implementation of meshed networks. Contextualizing mesh networks in CPPS, wireless network traffic is bridged from access point to access point, thereby reducing the need for ethernet cabling. Fig. 3 adapts the previous discussion of CPPS [7] to show IACS as a discrete safety function represented by the red boxes, necessary to control and contain hazardous processes.

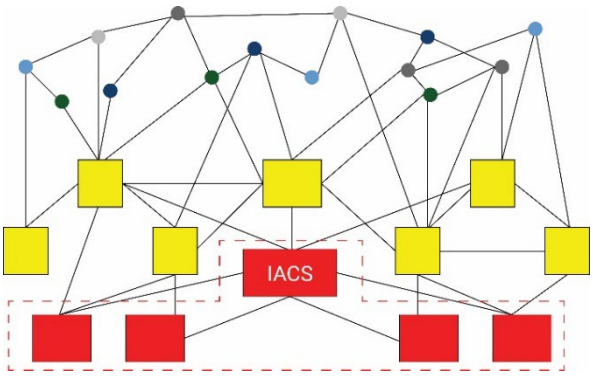

Fig. 3. CPPS meshed networks.

These safety-critical processes (red boxes) continue to be controlled by PLCs (Level 0), consistent with the practices set out in Fig. 2.A. The business-critical components, or modular CPPM that form the basis of CPPS, are shown in the yellow boxes. These will include the components supporting self-organization; e.g., re-configuration of packaging and dispatch functions appropriate to parcel sizes, or warehousing requirements as raw materials for draw-down arrive on the premises.

To manage risk in the self-organization paradigm, the safety-critical processes should be ring-fenced (red boxes in Fig. 3) such that if variation in a process requires further V&V to be completed, its function is left unvaried, and the non-critical functions are positioned around it to support asset optimization. If V&V needs to be performed, the benefits of CPPS self-organization may be reduced or negated. Moreover, this reduces the risk of CPPM exacerbating an existing hazard, the avoidance of which is a key tenet of IACS safety management [16].

The heterogenous nature and computation power of the devices within business-critical functions (yellow boxes in Fig. 3) may allow greater resilience in the business processes they support, through the addition of cost-effective CPPM-type redundant functions. Effectively, this is the business data equivalent of SIS supported by AI-type algorithms.

Also shown within the mesh environment in Fig. 3, as the circles above the business-critical functions, are the Fog, Cloud, and DLs endpoints that form part of the CPPS environment. These are third-party hosted services and will rely on AI algorithms to inform optimization. To secure data within IACS, operational networks are divided into zones, with data security policies specific to the security levels specified in IEC 62443, and appropriate to that zone's safety integrity requirements [23]. In Fig. 3, the red dashed line surrounding the red boxes reflects a Demilitarized Zone; physical or logical protection that treats the CMMP, Fog, Cloud, and DLs as untrusted entities, thereby limiting their data exchange and thus their control over the safety-critical functions.

To support CPPS-type mesh networks, research is underway to extend protocols such as LoraWan from star to mesh deployments. As the mesh network likely represents a further erosion of traditional network borders, the encryption key management weaknesses in LoraWan will also need to be addressed [28]. CIA vulnerabilities have been identified in the DDS middleware that orchestrates the integration [30]. Therefore, key security considerations raised by the Delphi panel include the suggestion that networks may need to move from IT-type security protections in business-critical DiD, to more data-centric models like Zero-Trust. In Zero-Trust, segmented zones are created at a host or data layer to enforce CIA within the CPPS model [10]. As the smart devices in Fig. 3 are computationally powerful, greater encryption can be applied at a granular level to data appropriate to their criticality, with encryption proportionate to the risk in that data, as well as the consumer of that data. Many Delphi panel participants noted that many businesses' security policies lack data classification and appropriate confidentiality mechanisms. To address this, encryption policies can be implemented based on classification across the smart devices, Mist, Fog, and/ or Cloud applications. Cumulatively these protections will bolster IT-type DiD, thereby reducing the risk of IT-type assets being used as the attack vector by threat-actors.

To assist the categorisation of controls that could account for data risks within a CPPS environment, the next section sets out factors that provide a wide range of IIoT generic security capabilities. Moreover, these factors are grouped under higher order properties (Reputation, Trust, and additionally Resilience) to assist transdisciplinary appraisal of the data risks and controls.

6. MODEL VALIDATION

This section sets out the inductive and exploratory techniques necessary to identify patterns relevant to CPSS data risk, based on the transdisciplinary panels information power [40]. To bring organizational context to the panellist's insights, the 24 interview transcripts were uploaded to a qualitative analysis tool. These key insights total 427, with AI accounting for 98 statements, DE 59, IT 118, and OT 152. Fig. 4 presents a word cloud based on a word frequency query across these 427 statements to show the dominant thematics.

As utility is a key objective of this research program, the panel was asked to confirm a set of attributes that can be used to group the risk controls relevant to CPPS and CPPM. The attributes applied in the initial round of the Delphi interviews were *Reputation* and *Trust* seeded from the directions in extant literature [1]. Initially *Resilience* was not included in the semi-structured questions put to panellists.

Fig. 4. Word cloud visualization of thematics.

Informing *Reputation* and *Trust* as possible attributes for discussion with the panel, were considerations drawn from a seminal IoT model [44], as well as IoT reference architectures [39] [45]. However, the expert insights considered resilience (as as bolded in black in Fig. 4) to be key as shown in Fig. 4, with *Reputation* less frequent (shown in grey). For the Legal & Risk cohort, *Resilience* and *Reputation* were primary attributes. In Fig. 4, *Trust* is shown as a dominant theme (based on word size within the diagram as well as being bolded in orange), primarily across the IT, AI, and in respect of process, the OT cohorts. In summary, all four cohorts consider these three attributes conferred a plain language context that can assist shared reference across transdisciplinary project teams.

The objectives of information systems inherent in these three attributes is summarized as:

- *Reputation*: That an entity integrated into the ecosystem can be relied upon to perform correctly, is authenticated so that confidentiality and integrity are maintained, and that the Thing(s) do not introduce vulnerabilities.
- *Resilience*: The ability to maintain critical operations, or recover from an impacted state. And can maintain the "5Cs: connection, conversion, cyber, cognition, and configuration" [2].
- *Trust*: That functions are performed correctly and through context-awareness, safety and integrity are maintained across sensors, actuators, algorithms, and networks.

Also forming part of the taxonomy resulting from this research are *Factors*. The taxonomical hierarchy flows as *Domain* → *Attribute* → *Factor*, where Factor refers to those elements that can be used both to classify the sources of risk, and under which grouping of risk control capabilities can be nested. In Section 2 under the IACS subsection, the difference between the discrete disciplines of IT and OT are set out. To identify the shared data security concerns across the IT and OT cohorts highlighted in grey in Table II are those factors that are shared factors (F1 – Identity, F7 – Communication Protocols, F8 – Energy, and F10 – Time & Consensus).

TABLE II. TAXONOMICAL FACTOR BASED ON DELPHI EXPERT OPINION

Reputation	Trust	Resilience
Auditing (F5)	Auditing (F5)	Auditing (F5)
Identity (F1)	Authentication (F3)	Data Classification (F9)
Inventory (F2)	Authorisation (F4)	Lifecycle Management (F6)
Lifecycle Management (F6)	Communication Protocols (F7)	Regulation & Compliance (F11)
Regulation & Compliance (F11)	Data Classifications (F9)	Time & Consensus (F10)
	Energy (F8)	
	Identity (F1)	
	Lifecycle Management (F6)	
	Time & Consensus (F10)	

To measure the level of agreement between the IT and OT cohorts regarding Factors common to both domains, Kendall's W was used as a measure of concordance. To assist measurement, during the initial Delphi round the IT and OT cohort were asked to rank the importance of the attribute on a 5-point Likert scale ranging from '*1 = Not Important At All*' to '*5 = Absolutely Essential*'. While this determined there was agreement between the practitioners across cohorts, challenging the use of model rank correlation typically associated with Likert scales is the fact that such measures assume equidistance between consecutive ranks. However, in Fig. 4 the words *need(s)* and *critical* reflect that the ranking between factors is implementation-specific; e.g., remote deployment of IoT sensors that inform business-critical data will emphasise energy, whereas those with mains power in a hazardous process industry may emphasize identity and authentication. Kendall's W was used as it does not include a restriction around the assumption that the distance between consecutive ranks is equidistant.

The risk factors identified in this research must be tactical, yet sufficiently generalised to provide for the containment of exploits not yet known, regardless of the severity they present. The next section presents the CPPS risk taxonomy including these Factors, based on the input of the of the next stage of the Delphi rounds.

7. FINDINGS

To further refine the model taxonomy, a closed questionnaire was sent to the 24 panellists to collect input covering the grouping of *Factors* under each *Attribute* as per Table II. To illustrate the resulting CPPS risk concepts, in Fig. 5 alongside the Attribute of *Reputation*, the *Factors* of *Identity*, *Asset Inventory*, *Regulations & Compliance*, are listed. Accompanying these *Factors* in Fig. 5 are a set of properties that are specific to that attribute's role in protecting the CPPS or CPPM's data assets.

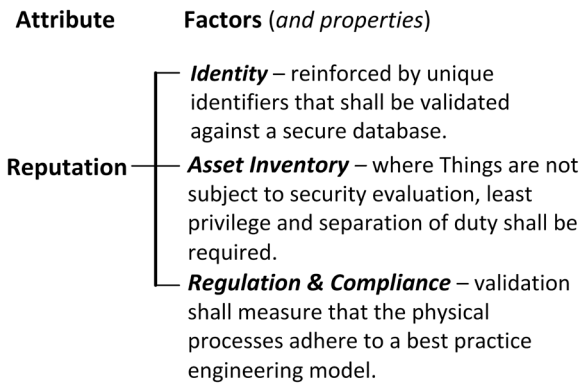

Fig. 5. Reputation Factors for CPPS Optimization.

Concepts relevant to Reputation in Table II included *Auditing,* but the panel input to the questionnaire was that *Auditing* is not a discrete activity, rather it is a function of *Verification & Validation* (with V&V discussed in Section 2). V&V was viewed as being necessary to meet the requirements of *Regulation & Compliance*, specifically that the behavior of the CPPS system and/ or CPPM agrees with its design.

In Fig. 6, supporting *Resilience* are *Factors* that while common to *Reputation* have a different contextual relevance. For example, *Regulation & Compliance* in *Resilience* addresses verification in V&V. Namely that the system meets its functional requirements, including safety. Also, Fig. 6 reflects the panel view that *Auditing* in terms of event and system logging is encapsulated in verification so is also a joined property of *Regulation & Compliance*. This satisfies the formal considerations tied to contractual requirements, and relevant to the Legal & Risk cohort. Namely, system service levels, Quality of Service (QoS), or more formal system recovery point and recovery time resilience type metrics applicable to measuring recovery from an impacted state.

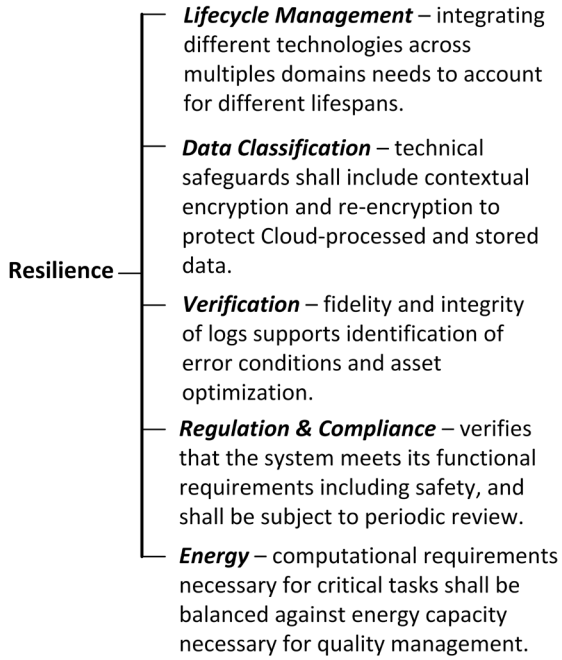

Fig. 6. Resilience Factors for CPPS optimization.

The panel considered that where *Reputation* and *Resilience* were present, the optimisation flowing from those attributes transfers to *Trust*. Therefore, in Fig. 7 the *Factors* that are shared across *Reputation* and *Resilience* are represented by these higher order categories (represented graphically by *Reputation* and *Resilience* being inputs to *Trust*). An example is *Identity*, where in the panel's views its relevance across the technical domains needs to account for the move from host-based authentication centred on IP addresses, to the world of service-based networking. In this service-driven

computation and networking paradigm, the service consumption models bought on by Mist, Fog, and multi-Cloud environments, require that user and device identify are bound to constant re-authentication as a core tenant of Zero-Trust. Therefore, as shown in Fig. 7 the panel view was that Trust is an oxymoron, and in fact Legal & Risk considerations should be looking for system capabilities where trust is never required. In essence: verify identity and authenticate…then trust.

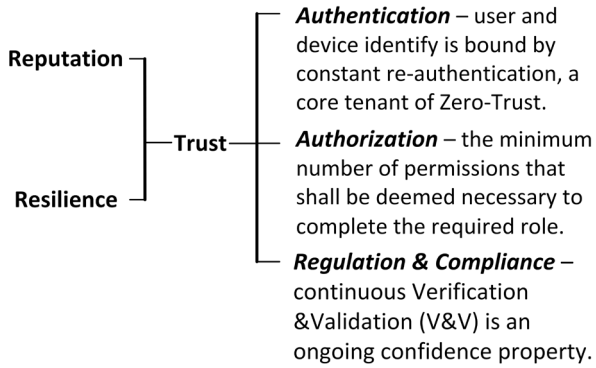

Fig. 7. Trust Factors for CPPS optimization.

To ensure utility in this taxonomy, technical security management capabilities based on a number of the synthesized themes in the extant literature are set out in Fig. 8. The *Capabilities* shown are specific to *Authorization*, discussed in Fig. 7 as a risk control factor that supports *Trust*.

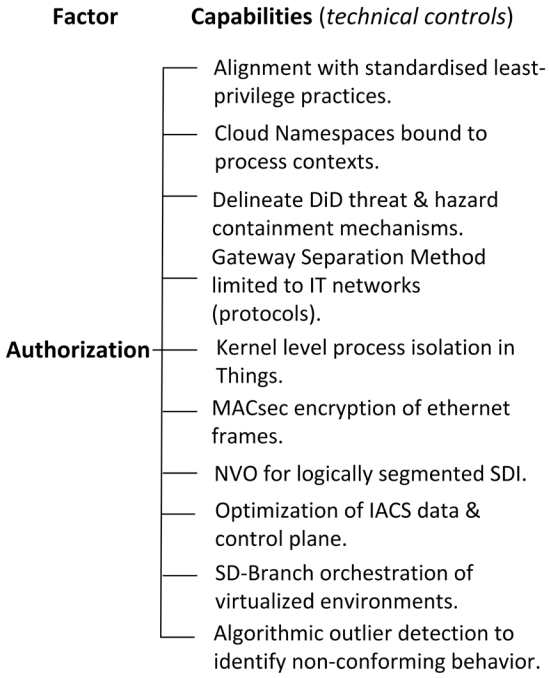

Fig. 8. Authorization capabilities.

The technical capabilities set out in Fig. 8 are from the literature using the systematic processes prescribed by PRISMA [1], and that were discussed in Section 3.

The addition of *Capabilities* extends the taxonomical hierarchal flows as *Domain* → *Attribute* → *Factor* → *Capabilities*.

The purpose of *Capabilities* is to capture the state of the art in generic security improvements and protections such as Network Virtualisation Overlay (NVO). To maintains state information at the edge of the network, NVO supports optimization of the underlying transport network necessary to measure and maintain contractual QoS legal and risk considerations. Such protections also include SD-Branch, an industry initiative for managing network complexity including increased IoT and Cloud traffic. Key functionality includes the discovery and/ or securing of Things, and SDI, or Software Defined Instructure, the categorization catch-all for SDN discussed in Section 1.

8. CONCLUSIONS, FUTURE RESEARCH

The introduction to this research explained that supporting CPPS and CPPM will be the 5Cs, which are centered around the adaption and flexibility of manufacturing processes [3]. Because CPPS is an emergent field within IIoT, 24 transdisciplinary experts knowledgeable in IT, OT, AI and Legal & Risk shared their expert views on directions in the technical domains and considerations that comprise CPPS, CPPM, and more broadly the IIoT. Following the interviews, themes were identified and coded, with the resulting insights reflecting data risk protections that can account for the hierarchical decomposition that characterizes emergent CPPS architectures. In Fig. 3 this decomposition of automation was extended to illustrate how integrated CPPS topologies will need to distinguish between safety-critical and business-critical tasks and the associated data risk. Delivering on the objectives of CPPS requires data to be fit for purpose in terms of ensuring resilient SAIC is maintained, and that the new technologies improve the information state of CIA.

In this research, it is noted that the fidelity of safety-critical and business-critical data necessary to support CPPS and broader Industry 4.0 type innovation, will likely challenge traditional IT-domain type DiD strategies. NIST [46] defines criticality "as the measure of the degree to which an organization depends on the information or information system". Therefore, the endpoints and nodes in Fig. 3 will need to support not only the critical functions implicit in reconfiguration, but also incorporate security protections given their integration within other CPS or CPPM may rely on the Internet as well as third-party computation services maintained by Mist, Fog, or Cloud providers. To assist shared reference across the transdisciplinary project teams that will be responsible for the implementation or maintenance of CPPS and IIoT assets, the three attributes

of Reputation, Resilience, and Trust are used to provide a plain language context under which a set of generalised data security factors can be ordered within a taxonomy.

By extending the conceptual CPPS model taxonomy, this research contributes to the emerging body of knowledge covering risk, and in particular the controls relevant to protecting a firm's dependency on the business-critical data that the CPPS system creates and consumes. As this research forms part of a program directed at developing methods that will help asset owners to enumerate data risk in emerging fields such as CPPS, the topics discussed in this research will be subject to further expert refinement.

The next phase of this research will develop the final research artefact that captures the classes of risk protections appropriate to DiD across the multidisciplinary CPPS domain within IoT. This will inform support for the business-critical data boundaries that production systems will need to to re-organize around, particularly where hazardous processes may be present.

9. ACKNOWLEDGMENTS

We cannot adequately express our gratitude to the Delphi experts who willingly gave up their time to participate in this research. Given their professional standing and expertise, taking time out of their busy schedules to share their views was extremely generous. Our thanks also go to the peer review editors who gave of their time to evaluate and comment on this journal paper.

10. REFERENCES

[1] G. Ward and L. Janczewski, "Using Knowledge Synthesis to Identify Multi-dimensional Risk Factors in IoT Assets," in **Third International Conference on Advances in Cyber Security**, Singapore, 2021: Springer, in Advances in Cyber Security, pp. 176-197, doi: 10.1007/978-981-16-8059-5_11.

[2] British Standards, "ISO/IEC TR 30166:2020 Internet of things (IoT). Industrial IoT," in "PD ISO/IEC TR 30166:2020," BSI Standards, London, 2020.

[3] T. Müller, N. Jazdi, J.-P. Schmidt, and M. Weyrich, "Cyber-physical production systems: enhancement with a self-organized reconfiguration management," **Procedia CIRP, vol. 99**, pp. 549-554, 2021, doi: 10.1016/j.procir.2021.03.075.

[4] G. Schuh, R. Anderl, R. Dumitrescu, A. Krüger, and M. ten Hompel, "**Industrie 4.0 Maturity Index. Managing the Digital Transformation of Companies – UPDATE 2020**," acatech National Academy of Science and Engineering,, 2020.

[5] H. A. Khattak, M. A. Shah, S. Khan, I. Ali, and M. Imran, "Perception layer security in Internet of Things," Future Generation Computer Systems, vol. 100, pp. 144-164, 2019, doi: 10.1016/j.future.2019.04.038.

[6] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial Internet of Things: Challenges, Opportunities, and Directions," **IEEE Transactions on Industrial Informatics**, vol. 14, no. 11, pp. 4724-4734, 2018, doi: 10.1109/TII.2018.2852491.

[7] Y. Lu, K. Morris, and S. Frechette, "Current Standards Landscape for Smart Manufacturing Systems," NIST, Maryland, 2016, vol. NISTIR 8107.

[8] K. S. Sahoo, M. Tiwary, A. K. Luhach, A. Nayyar, K. K. R. Choo, and M. Bilal, "Demand-Supply Based Economic Model for Resource Provisioning in Industrial IoT Traffic," **IEEE IoT Journal**, pp. 1-1, 2021, doi: 10.1109/JIOT.2021.3122255.

[9] IEEE, "IEEE Standard for Adoption of OpenFog Reference Architecture for Fog Computing," IEEE Std 1934-2018, pp. 1-176, 2018, doi: 10.1109/IEEESTD.2018.8423800.

[10] M. J. Haber, **Privileged Attack Vectors: Building Effective Cyber-Defense Strategies to Protect Organizations**, 2nd ed. Berkeley: Apress, 2020, pp. 295-304.

[11] D. Yu, Y. Jin, Y. Zhang, and X. Zheng, "A survey on security issues in services communication of Microservices-enabled fog applications," **Concurrency and Computation**, vol. 31, no. 22, 2019, doi: 10.1002/cpe.4436.

[12] L. Wang and X. V. Wang, "Latest Advancement in CPS and IoT Applications," in **Cloud-Based Cyber-Physical Systems in Manufacturing**. Switzerland: Springer, 2018.

[13] ISO/IEC JTC 1/SC 42. "Standards by JTC 1/SC 42 - Artificial intelligence." www.iso.org (accessed 12 November 2021.

[14] Congnizant. "Case Studies." www.cognizant.com (accessed 28 January 2022.

[15] E. Pricop, J. Fattahi, N. Dutta, and M. Ibrahim, **Recent developments on industrial control systems resilience**. Switzerland: Springer, 2020.

[16] British Standards, "BS EN ISO/IEC 27001:2017 Information technology. Security techniques. Information security management systems. Requirements," BSI Standards, London, 2017, vol. BS EN ISO/IEC 27001:2017.

[17] IIC, "Industrial Internet of Things Volume G4: Security Framework," Industrial Internet Consortium, Massachusetts, 2016, vol. V1.0:PB:20160926. [Online]. Available: iiconsortium.org

[18] A. Hahn, "Operational Technology and Information Technology in Industrial Control Systems," in **Cyber-security of SCADA and Other Industrial Control Systems**, E. J. M. Colbert and A. Kott Eds.

Switzerland: Springer, 2016, pp. 51-68.
[19] E. A. Lee, "What are the key challenges in embedded software," **System Design Frontier**, vol. 2, no. 1, p. 13, 2005.
[20] UC Berkeley. "System Validation and Verification Plans." https://connected-corridors.berkeley.edu (accessed 21 October 2021.
[21] P. Marwedel, **Embedded System Design**, 3rd ed. Switzerland: Springer, 2017.
[22] Functional safety - Safety instrumented systems for the process industry sector, Standard PD CLC IEC/TR 61511-4:2020, British Standards, London, 2020.
[23] J.-M. Flaus, **Cybersecurity of industrial systems**. London: Wiley, 2019.
[24] D. E. Sanger, "Hack of Saudi Petrochemical Plant Was Coordinated From Russian Institute," in The New York Times, ed. New York, 2018.
[25] Dragos, "TRISIS Malware Analysis of Safety System Targeted Malware," 2018, vol. 1.20171213. [Online]. Available: www.dragos.com
[26] J. R. Reeder and T. Hall, "Cybersecurity's Pearl Harbor Moment: Lessons Learned from the Colonial Pipeline Ransomware Attack," 2021.
[27] NIST. "Glossary of Key Information Security Terms." NIST. https://csrc.nist.gov/glossary (accessed 8 January 2021.
[28] S. Figueroa-Lorenzo, J. Añorga, and S. Arrizabalaga, "**A Survey of IIoT Protocols: A Measure of Vulnerability Risk Analysis Based on CVSS**," ACM, vol. 53, no. 2, p. Article 44, 2020, doi: 10.1145/3381038.
[29] LoRa Alliance. "Full End-To-End Encryption For IoT Application Providers." LoRa Alliance. http://lora-alliance.org (accessed.
[30] CISA, "Multiple Data Distribution Service (DDS) Implementations," 11 November 2021 2021.
[31] E. Kovacs, "IoT Protocol Used by NASA, Siemens and Volkswagen Can Be Exploited by Hackers," 15 November 2021 2021. [Online]. Available: www.securityweek.com.
[32] M. Botterman, J. Cave, and A. Doria, "Standardization Issues," in **ICT Policy, Research, and Innovation**, 2020, pp. 309-330.
[33] G. Ward and L. Janczewski, "Investigating Data Risk Considerations in Emergent Cyber Physical Production Systems," in Proceedings of the **13th International Multi-Conference on Complexity, Informatics and Cybernetics: IMCIC 2022**, Florida, P. N. Callaos, Ed., 2022, doi: 10.54808/IMCIC2022.02.119.
[34] ISO. "ISO/DIS 23704-1: General requirements for cyber-physically controlled smart machine tool systems (CPSMT) — Part 1: Overview and fundamental principles." www.iso.org (accessed 21 October 2021.
[35] G. Paré, A.-F. Cameron, P. Poba-Nzaou, and M. Templier, "A systematic assessment of rigor in information systems ranking-type Delphi studies," **Information & Management**, vol. 50, no. 5, pp. 207-217, 2013, doi: 10.1016/j.im.2013.03.003.
[36] A. Alarabiat and I. Ramos, "The Delphi Method in Information Systems Research (2004-2017)," **Electronic Journal of Business Research Methods**, vol. 17, no. 2, p. 86-99, 2019, doi: 10.34190/JBRM.17.2.04.
[37] V. Braun and V. Clarke, "Using thematic analysis in psychology," **Qualitative research in psychology**, vol. 3, no. 2, pp. 77-101, 2006.
[38] E. A. Lee and S. A. Seshia, **Introduction to Embedded Systems : A Cyber-Physical Systems Approach**, Second Edition, Version 2.2 ed. Massachusetts: MIT Press, 2017.
[39] IERC, "IoT Governance, Privacy and Security Issues," in "European Research Cluster on the Internet of Things," IoT European Research Cluster, Oslo, 2015. [Online]. Available: www.internet-of-things-research.eu
[40] H. Khujamatov, E. Reypnazarov, D. Khasanov, and N. Akhmedov, "IoT, IIoT, and Cyber-Physical Systems Integration," in **Emergence of Cyber Physical System and IoT in Smart Automation and Robotics: Computer Engineering in Automation**, K. K. Singh, A. Nayyar, S. Tanwar, and M. Abouhawwash Eds. Switzerland: Springer, 2021, pp. 31-50.
[41] J.-P. A. Yaacoub, O. Salman, H. N. Noura, N. Kaaniche, A. Chehab, and M. Malli, "Cyber-physical systems security: Limitations, issues and future trends," **Microprocessors and Microsystems**, vol. 77, p. 103201, 2020, doi: 10.1016/j.micpro.2020.103201.
[42] The Economist, "Huge "foundation models" are turbo-charging AI progress," AI, 11 June 2022. [Online]. Available: www.economist.com
[43] G. Bloom, B. Alsulami, E. Nwafor, and I. C. Bertolotti, "Design patterns for the industrial Internet of Things," in 2018 **14th IEEE International Workshop on Factory Communication Systems**, 2018, pp. 1-10, doi: 10.1109/WFCS.2018.8402353.
[44] ITU, "Overview of the Internet of things," in "Telecommunication Standardization Sector," International Telecommunication Union, Geneva, 2012, vol. ITU-T Y.2060. [Online]. Available: www.itu.int
[45] IIC, "The Industrial Internet of Things - Volume G1: Reference Architecture," Industrial Internet Consortium, Massachusetts, 2019, vol. IIC:PUB:G1:V1.80:20170131. [Online]. Available: www.iiconsortium.org
[46] Guide for Mapping Types of Information and Information Systems to Security Categories, NIST, Maryland, 2008.