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

ABSTRACT

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 flow across the CPPS model. The resulting refinements to current models were informed by a 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. 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].

Self-organization

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 fulfill a certain function, or can be reconfigured to achieve another function. These Cyber Physical Production Modules (CPPM) will consist of heterogenous components [3].

Supporting this continual data analysis are more computationally powerful smart actuator and sensor devices connected to Fog and the Cloud, which utilize 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. The use of these technologies will bring flexibility to the hierarchies that characterize manufacturing automation [5]. Assisting flexibility are Software Defined Networks (SDN), a relatively new network paradigm that supports the logical centralization of physically distributed hardware in software [6]. In SDN, the software backplane uses virtualization to support scalability and improve security through process isolation, micro segmentation [7], and Zero-Trust [8]. Additionally, many CPPM applications may utilize 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 [9].

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 IIoT.

Challenging precision in defining CPPS within IIoT is that its use-cases are a "thematic subject as opposed to a disciplinary topic" [10]. While emerging from IT and electrical engineering, [10] 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 [11]. Those under development include the use of AI in standards such as *Functional safety and AI systems*, as well as *Risk Management* [11], which are relevant to 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

ISBN: 978-1-950492-61-9
ISSN: 2771-5914

https://doi.org/10.54808/IMCIC2022.02.119

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 [12], 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 [12]. Extending these case-studies into increasingly more complex self-organizing paradigms across multiple manufacturing categories, 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. The expert input of a panel of IT and OT experts informed the refinement of the conceptual model alongside key risk considerations. The objective of this research is to contribute to the development of a systems approach to risk assessment in CPPS.

This research is structured as follows. Section 2 discusses the evolution of Industrial Automation and Control Systems (IACS) as well as key data considerations and the current state of standardization. Section 3 sets out the methodology used in this research. Section 4 brings specificity to where CPPS sits within the IIoT paradigm, and in section 5 the findings show how traditional data hierarchies will flatten as the management of business-critical data is supported by new technologies. Section 6 presents the research conclusions.

2. IIOT PROCESS DATA

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 they are key to process correctness, followed by Confidentiality (AIC) [1]. For 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.

The common usage of the word *critical* implies both the significance and consequences of failings, relating specifically to matters "of the greatest importance to the way things might happen" and "extremely serious or dangerous" [13]. 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 CSSP 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 [14].

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 with differences including:

- Separate architectures: the two domains have different computational priorities in that OT emphasizes process correctness, whereas IT emphasizes performance [17].
- Communication protocols: conflicting protocols may cause OT systems to enter an unsafe state [18].
- 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 [19].
- Divergent design: safety is a critical OT design criterion [18], whereas IT prioritizes confidentiality and integrity.
- Hardware versus software: traditionally IT has favored software security protections, and OT has favored hardware [18].

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 [20]. Validation examines the processes used to determine that the right system was built, and the resulting behavior of the physical system [21]. Verification is used to ensure the system meets its functional requirements, including safety [21]. 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 [22]. 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 [22].

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 [23]. 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 [24]. 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 risks to SIS, in 2017, nation state actors compromised an SIS installed in a Saudi Arabian oil refinery [25]. 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 [26]. It is considered that TRISIS was likely installed following a compromise of the intermediatory IT networks used for remote access to the IACS [26]. 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 failings 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 [27]. 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 [28]. 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 [29] 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 [30]. LoraWan's security includes each smart device using robust AES data encryption, and globally unique identifiers to support device identity management [30]. However, weaknesses include encryption key management using long-term keys, and encryption functions relying on repetitive cipher patterns [29].

Illustrating threats, in late 2021 a key US cyber agency, CISA [31], 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 [31]. This middleware has been implemented by NASA, Siemens, and Volkswagen [32].

Standardization of Other Core Technologies

As set out in the previous section, with 72% of AI-related standards currently under development [11], this may challenge the V&V of systems, given the absence of uniform standards. As risk management is used to reduce inherent risk to be within organizationally acceptable tolerances, the absence of standardization could result in adverse variance within the inherent risk.

Developing standards is a time-consuming process for SDOs. For example, standardizing 5G specifications spanned 5 years (2015 through 2020) [33]. 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" [33] [5].

To illustrate the complexity IIoT presents risk managers, Fig. 1 shows standards that may be applicable (subject to the extent of safety-critical considerations). An asterisk (*) next to a standard indicates it is currently under development. While Fig. 1 does not provide an exhaustive list of standards that may be relveant to IIoT, it illustrates the plethora of standards that the heavily integrated fields of IIoT and CPPS may need to satisfy as part of robust V&V processes.

For example, key aspects of IEC TR 30166 covering IIoT [2] that are still drafts include AI [2]. While AI is noted as enabling sustained autonomous operations, it is subject to evaluation by other SDOs [2]. And while CPPS is referenced, there is no specificity [2]. Also, in Fig. 1, included under *Cyber Physical Production Systems* are two parts of the ISO 23704 series addressing *Cyber-Physically controlled Smart Machine Tools*. While this series may inform CPPM, as drafts they are yet to be ratified [34].

Information Technology		**Operational Technologies**	IEC 61158	Industrial communication networks
IEC 27000	Security techniques.		IEC 61850	Communication networks and systems for power utility automation
IEC 17799	Security techniques — Code of practice for information security management		IEC 61511	Functional safety - Safety instrumented systems for the process industry sector
IEC TS 23167	Cloud computing - Common technologies and techniques		IEC 61508	Functional safety of electrical/electronic/programmable electronic safety-related systems
SP 800-60	Guide for Mapping Types of Information and Information Systems to Security Categories		NIST SP 800-82	Guide to Industrial Control Systems (ICS) Security
Artificial Intelligence			IEC 61512	Batch control
IEC CD 23894*	Risk Management		IEC TR 62443	Security for Industrial Automation and Control Systems (IACS)
IEC CD 42001*	Management system		IEC 62264	Enterprise-control system integration
IEC AWI TR 5469*	Functional safety and AI systems	**IoT & IIoT**	IEC TR 30166	Internet of things (IoT). Industrial IoT.
IEC TR 24029-2*	Assessment of the robustness of neural networks (methodology - pt 2)		IEC TS 23167	Information technology - Cloud computing - Common technologies and techniques
IEC TR 20547	Big data reference architecture and application process		ISO 30162*	Compatibility requirements and model for devices within industrial IoT systems
IEC TR 24028	Overview of trustworthiness in artificial intelligence		IEC 30141	Internet of Things (IoT) — Reference Architecture
Cyber Physical Production Systems				
ISO 23704-1*	General requirements for cyber-physically controlled smart machine tool systems (CPSMT). Part 1. Overview and fundamental principles			
ISO 23704-2*	General requirements for cyber-physically controlled smart machine tool systems (CPSMT). Part 2. Reference architecture of CPSMT for subtractive manufacturing			

* Standards under development.

Fig. 1. Standards relevant to IIoT and CPPS.

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. DEFINING MODEL ATTRIBUTES

Alongside the literature cited in this research, the IACS, CPS, and risk considerations discussed have been shaped by the insights of 18 heterogenous experts, including those with domain expertise across IT, IACS, and IoT. Using the research method Delphi, expert opinion covering risk attributes in the IIoT integration cores has been 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 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 18 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 depth of experience across the IT participants spanned operations and security architects, breach response, and risk consulting, with an average of 25 years of practice. The OT and IoT participants' experience spanned industrial cyber security, electrical and mechanical engineering, and academia, with an average of 19 years of practice. Research ethics permission was obtained from the authors' academic institutions prior to this research commencing, and participants consented to their contributions being included in this research. Interviews lasted between 75 and 120 minutes.

4. IIOT INTEGRATION

CPPS within the IIoT Ecosystem

Fig. 2 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.

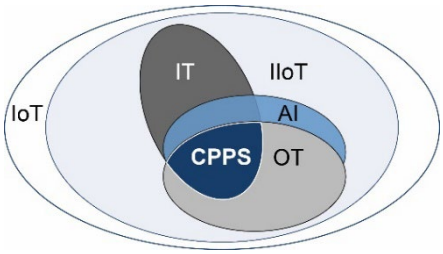

Fig. 2. CPPS, the intersection of technologies.

Directions in the literature suggest that CPS behavior can achieve reliability through the use of error-correction algorithms, relying on a learned state acquired through Machine Learning (ML) [37]. However, as shown in Fig. 1, AI-related standards such as *Functional safety and AI systems*, and the methodology for *Assessment of the robustness of neural*

networks, are under development. Furthermore, as ML is often viewed as a black box function, verification can be difficult. Where the 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. This panel view is that the absence of standardization is a current constraint on uptake.

Smart devices refer to powerful microcontroller units that may include a central processor, memory, and have Real Time Operation Operating Systems (RTOS) installed, which can support algorithms, as well as inbuilt sensors and actuators. The smart devices are Internet enabled for communication with Fog and Cloud [38]. The algorithms can support self-determination, including 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].

Comparison of CPS and IIOT

To assist the categorization of CPPS and IIoT, 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	Emergent device	IT practices
	Management	practices.	
Control	Functional objective	Physical process	Asset optimization

In Table I, Micro describes functions concerned with specific processes or device clusters, whereas Macro refers to the entire IIoT ensemble as shown in Fig. 2.

The view of the Delphi panel is that the goal of adaptive, self-configuring, and self-organizing systems will necessitate change in the hierarchical automation architecture that specifies IACS integration. Future directions are elaborated in the next section.

5. CPPS DATA MODEL

Standardized Safety-Critical

Fig. 3.A shows a four-layer representation of the ISA-95 Automation Pyramid that generalizes IACS deployments. ISA-95 is ratified under IEC 62264 as shown in the OT quadrant of Fig. 1. The Automation Pyramid (pyramid) is applicable to manufacturing processes, whether they are hazardous or not. In Fig. 3.B the pyramid is adapted following panel feedback.

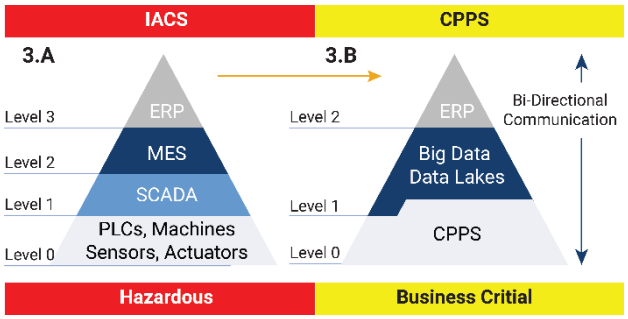

Fig. 3. CPPS compression of the Automation Pyramid.

In the traditional pyramid presented in Fig. 3.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). The DCS supports data collection, analysis, and presentation of control information to human operators [41]. In Fig. 3.A, at Level 2 data is further aggregated in the Manufacturing Execution System (MES), which assists production planning [24]. 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. 3.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 3.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. 3.B illustrates the compression of hierarchies, in this research Fig. 4 extends the decomposition of automation [5] 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. 4 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. 4 adapts the previous discussion of CPPS [5] to show IACS as a discrete safety function represented by the red boxes, necessary to control and contain hazardous processes.

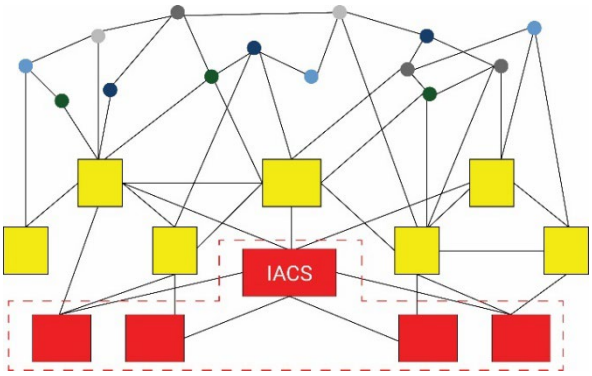

Fig. 4. CPPS meshed networks.

These safety-critical processes (red boxes) continue to be controlled by PLCs (Level 0), consistent with the practices set out in Fig. 3.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. 4) 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. 4) 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. 4, 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 [24]. In Fig. 4, 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 [42] 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 [29]. CIA vulnerabilities have been identified in the DDS middleware that orchestrates the integration [31]. 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 [8]. As the smart devices in Fig. 4 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, Fog, Cloud, and DLs applications. Cumulatively these protections will bolster I-type DiD, thereby reducing the risk of IT-type assets being used as the attack vector by threat-actors.

6. CONCLUSIONS, FUTURE RESEARCH

The introduction detailed the 5Cs in CPPS, centered on supporting adaption and flexibility in manufacturing processes [3]. Because CPPS is an emergent field within IIoT, 18 heterogenous experts knowledgeable in IT, IACS, and IoT provided opinions on directions in CPPS, based on semi-structured questions seeded from literature. Following the interviews, themes were coded, and the traditional Automation Pyramid was adapted to account for the hierarchical decomposition that emergent CPPS architectures will support (Fig 3.B). Additionally, prior work showing the decomposition of automation [5] was extended to better account for both safety-critical and business-critical data risk, given the co-dependency risks that the CPPS integration model must provide for (Fig. 4).

CPPS represents a conceptual paradigm for optimizing manufacturing, in which traditional hierarchies are replaced with more data-centric models. Realization of these objectives requires data to be fit for purpose in terms of ensuring robust SAIC is maintained, and that the new technologies improve the information state of CIA. In this research, these objectives are classified as safety-critical or business-critical respectively, for

which the former in particular challenges traditional IT-type DiD strategies. NIST [43] defines criticality "as the measure of the degree to which an organization depends on the information or information system". Therefore, this research, by extending the conceptual CPPS model, contributes to the emerging body of knowledge covering risk, and the methods that will be used to measure a firm's dependency on that CPPS system.

As this research forms part of a program directed at developing methods that can help asset owners to enumerate risk in emerging fields such as CPPS, the topics discussed in this research will be subject to further expert refinement. This future refinement will progress the objective of developing a systematic design for evaluating risk in CPPS, as well as identifying the classes of risk protections appropriate to DiD across the multidisciplinary IIoT domain.

This future scope of work will include the composition of the meshed networks to inform delineation of process boundaries necessary for production systems to re-organize around hazardous processes. This will assist the evaluation of risk necessary to ensure the integrity of safety-critical IACS processes, while optimizing the availability of business-critical data that IoT and CPS support.

7. 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 Singapore, 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. Available: https://en.acatech.de/publication/industrie-4-0-maturity-index-update-2020/

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

[6] 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 Internet of Things Journal**, pp. 1-1, 2021, doi: 10.1109/JIOT.2021.3122255.

[7] 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.

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

[9] 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: Practice and Experience**, vol. 31, no. 22, 2019, doi: 10.1002/cpe.4436.

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

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

[12] Congnizant. "Case Studies." https://www.cognizant.com/us/en/case-studies (accessed 28 January 2022.

[13] Cambridge. "Dictionary." dictionary.cambridge.org (accessed 21 October 2021.

[14] ISA. "Industrial Automation and Control System Taxonomy." gca.isa.org (accessed 3 October 2021.

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

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

[17] P. Lara, M. Sánchez, and J. Villalobos, "OT Modeling: The Enterprise Beyond IT," Business & Information Systems Engineering, journal article vol. 61, no. 4, pp. 399-411, August 01 2019, doi: 10.1007/s12599-018-0543-3.

[18] IIC, "Industrial Internet of Things Volume G4: Security Framework," Industrial Internet Consortium, Massachusetts, 2016, vol. IIC:PUB:G4:V1.0:PB:20160926. [Online]. Available: iiconsortium.org/pdf/Industrial_Internet_of_Things_Volume_G2-Key_System_Concerns_2018_08_07.pdf

[19] 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. Cham, Switzerland: Springer, 2016, pp. 51-68.

[20] E. A. Lee, "What are the key challenges in embedded software," **System Design Frontier**, vol. 2, no. 1, p. 13, 2005.

[21] UC Berkeley. "System Validation and Verification Plans." connected-corridors.berkeley.edu/developing-system/system-validation-and-verification-plans (accessed 21 October 2021.

[22] P. Marwedel, **Embedded System Design**, 3rd ed. 6330 Cham, Switzerland: Springer, 2017.

[23] Functional safety - Safety instrumented systems for the process industry sector, Standard PD CLC IEC/TR 61511-4:2020, British Standards, London, 2020.

[24] J.-M. Flaus, **Cybersecurity of industrial systems**. London: Wiley, 2019.

[25] D. E. Sanger, "Hack of Saudi Petrochemical Plant Was Coordinated From Russian Institute," in The New York Times, ed. New York: The New York Times, 2018.

[26] Dragos, "TRISIS Malware Analysis of Safety System Targeted Malware," 2018, vol. 1.20171213. [Online]. Available: www.dragos.com

[27] J. R. Reeder and T. Hall, "Cybersecurity's Pearl Harbor Moment: Lessons Learned from the Colonial Pipeline Ransomware Attack," 2021.

[28] NIST. "Glossary of Key Information Security Terms." NIST. https://csrc.nist.gov/glossary (accessed 8 January 2021.

[29] 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.

[30] LoRa Alliance. "Full End-To-End Encryption For IoT Application Providers." LoRa Alliance. lora-

alliance.org/sites/default/files/2019-05/lorawan_security_whitepaper.pdf (accessed.

[31] CISA, "Multiple Data Distribution Service (DDS) Implementations," 11 November 2021 2021. [Online]. Available: us-cert.cisa.gov/ics/advisories/icsa-21-315-02.

[32] E. Kovacs, "IoT Protocol Used by NASA, Siemens and Volkswagen Can Be Exploited by Hackers," 15 November 2021 2021. [Online]. Available: www.securityweek.com/iot-protocol-used-nasa-siemens-and-volkswagen-can-be-exploited-hackers.

[33] M. Botterman, J. Cave, and A. Doria, "Standardization Issues," in **ICT Policy, Research, and Innovation**, 2020, pp. 309-330.

[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/obp/ui#iso:std:iso:23704:-1:dis:ed-1:v1:en (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] 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.

[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: Engineering in Automation**, K. K. Singh, A. Nayyar, S. Tanwar, and M. Abouhawwash Eds. Switzerland: Springer, 2021, pp. 31-50.

[41] 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 (WFCS), 13-15 June 2018 2018, pp. 1-10, doi: 10.1109/WFCS.2018.8402353.

[42] J. R. Cotrim and J. H. Kleinschmidt, "LoRaWAN Mesh Networks: A Review and Classification of Multihop Communication," (in eng), Sensors, vol. 20, no. 15, p. 4273, 2020, doi: 10.3390/s20154273.

[43] Guide for Mapping Types of Information and Information Systems to Security Categories, NIST, Maryland, 2008.