Towards Adaptive Inspection for Fraud in I4.0 Supply Chains

*Thomas Welsh, *Faeq Alrimawi, *Ali Farahani *Diane Hassett, †Andrea Zisman, *†Bashar Nuseibeh
*University of Limerick, Ireland †The Open University, UK
firstname.lastname@{*ul.ie||†open.ac.uk}

***Abstract*—The effective functioning of society is increasingly reliant on supply chains which are susceptible to fraud, such as the distribution of adulterated products. *Inspection* is a key tool for mitigating fraud, however it has traditionally been constrained by physical characteristics of supply chains such as their size and geographical distribution. The increasingly cyber-physical nature of supply chains, their autonomy, and their data richness, extends their attack surfaces and thus increases opportunities for fraud. However, it also presents new opportunities for increased and dynamic inspection, which in turn requires more targeted and flexible inspection regimes. In this paper we explore opportunities to engineer *adaptive inspection* of cyber-physical supply chains to support efforts to reduce fraud. Through using structural representations of supply chains (topological models) we propose defining optimal *inspection zones*. Such zones circumscribe assets of interest to optimise observation while reducing the intrusiveness of inspection. Using a motivating example of adulterated pharmaceuticals and a proof-of-concept tool we illustrate adaptive inspection, and surface challenges to its realisation, such as value metrics, forensic readiness integration and managing contrasting local and global perspectives.**

***Index Terms*—adaptive, inspection, fraud, I4.0, supply chains,**

I. Introduction

A Supply Chain (SC) comprises a network of entities that collaborate to achieve the manufacturing and sale of a product: mining raw materials and their refinement, manufacturing and integration, and the distribution and sale of the final product to the end consumer. Recent global events including the COVID19 pandemic and turbulent political environments have highlighted the fragility of SCs, and illustrated how dependent society is upon their effective operation.

Unfortunately, SCs are known to suffer widely from fraud: food [1], medicines [2] and electronics [3] SCs are common victims. Fraud is a deceptive transfer of value [4], occurring where observation and controls fail. Increasing globalisation and the multitude of precursors required for modern products creates layered networks of producers and consumers which span the globe [2]. This complexity increases the area for observation and therefore the deception attack surface, creating an environment conducive to fraud. One technique used to increase observation is *inspection*. Usually conducted for quality, security, maintenance and audit, inspection may also be used to detect fraud. However, inspection techniques are resource intensive, and current solutions attempt to optimise strategies with a cost-based objective function [5]. While inspection of traditional supply chains is constrained by their physical characteristics, the data present in cyber-physical supply chains presents opportunities for less-constrained inspection. However, supply chains are *evolving* alongside the emergence of an industrial transformation: *Industry 4.0 (I4.0)*. The driving force behind this transformation is enhanced technological *integration*; not simply from the perspective of the SC, but also its *value chain* (VC), which reflects all value creating business processes and services [6]. I4.0 can be considered as *a way in which value chains are transformed to become more integrated with customers' needs* [7] [8]. Horizontal, vertical, and end-to-end integration across the complete value chain are becoming both possible and inevitable [6] [9]. This data rich integration permits autonomous and agile SCs that are able to react to market dynamics and stronger customer involvement required to remain competitive. As these variable markets influence the value of the SC assets, there is a need for more dynamic approaches to inspection. This introduces new attack vectors and threats to I4.0 environments, giving rise to novel forms of fraud that exploit these characteristics. The I4.0 community has identified the dynamic structure and autonomous decentralised management as key challenges to the future of I4.0 SC and its security and, therefore, for the mitigation of novel kinds of fraud [10] [6].

In this paper, we propose *adaptive inspection* to reflect such dynamism. Building on our previous work on both asset-centric adaptive security [11] and privacy zones [12], we propose *inspection zones* to dynamically circumscribe assets of interest and provide more effective inspection. The goal of our approach is to achieve asset-centric adaptive inspection to accommodate complex value networks inherent to the supply chains of the future.

The rest of this paper is structured as follows: Section II presents a motivating example of adulterated pharmaceuticals. Section III provides a background of fraud in supply chain, supply chain quality inspection, and future I4.0 supply chains. Section IV proposes a topology-aware adaptive inspection approach. Section V illustrates a running example with a proof-of-concept and discusses challenges to its realisation. Section VI concludes the work.

II. Globalised Pharmaceutical SC Example

To motivate to our work, in this section we present an example of globalised pharmaceutical SC based on the study in [2]

978-1-7281-2989-1/21̇0̇0

and illustrated in fig. 1. The materials, Active Pharmaceutical Ingredients (API)s, are produced in East Asia (e.g. China), the pharmaceuticals are manufactured elsewhere (e.g. India), and then distributed for consumption worldwide. Packaging and repacking occurs continuously throughout the chain. In wealthy countries, large multi-nationals control the market; while in lower and middle-economy countries the market contains thousands of actors and control is decentralised. This environment is highly dynamic to meet varying global demand. Therefore, information regarding the SC and its actors is generally opaque to most.

The SC actors will supply numerous jurisdictions with different quality and regulatory standards, which have associated differences in value. For example, increasing the level of an API to World Health Organisation standards can double the cost of a product meant for a nation with less strict requirements. Furthermore, while the industry is strongly regulated in wealthy nations, regulation is extremely difficult in larger, dynamic markets, due to costs required to operate at larger scales in nations with comparatively low financial resources. Inspection resource issues are particularly pertinent due to the high complexity of this environment, and the lack of motivation for producers to inspect, given the high cost and low regulation. These factors cause products to frequently mix across jurisdictions. Where products are of inferior quality through negligence and adulteration, or are counterfeit due to unethical use of packaging, products will be distributed fraudulently. Fraud is driven by the economic motivations to compete in this dynamic market. Fraud is also enabled through poor observability of the SC structure, actors and asset movements as a result of the highly complex environment and divergences in manufacturing culture, languages and standards.

To provide inspection for mitigating fraud within this environment, solutions would require accurate information about the supply chain structure to determine the target of inspection. Further information would be required regarding the assets within that target (such as the machinery, staff, and movement of goods) in order to determine the inspection policy. All of these issues are even more complicated through the SC geospatial-distribution causing inspection to be uneconomical.

We consider automated cyber-physical inspection approaches within I4.0 environments as a solution. We highlight three key requirements: *Data availability* to describe the SC structure, its processes and assets; *SC Modelling* techniques for inspection analysis; and techniques for *Inspection Planning* to determine the optimal time and place to inspect given constraints.

III. Background

In this section we review the notion of fraud in general and relate it to SC fraud in particular; we also present background on SC quality inspection and some on I4.0 SCs.

A. Fraud in Supply Chains

Fraud is an activity in which value is transferred from one party to another through deceptive means [4]. The target of this transfer is an *asset* which holds a perceived social or financial value to both parties. Fraud is instigated by one or more collaborating *deceivers* against one or more *victims*, be they natural persons or organisational entities such as companies, NGOs or governments. *Drivers* of fraud are commonly tangible economic reasons such as financial manipulation or to bypass regulation. They may also be intangible due to culture, high complexity, or irrational behaviour [13].

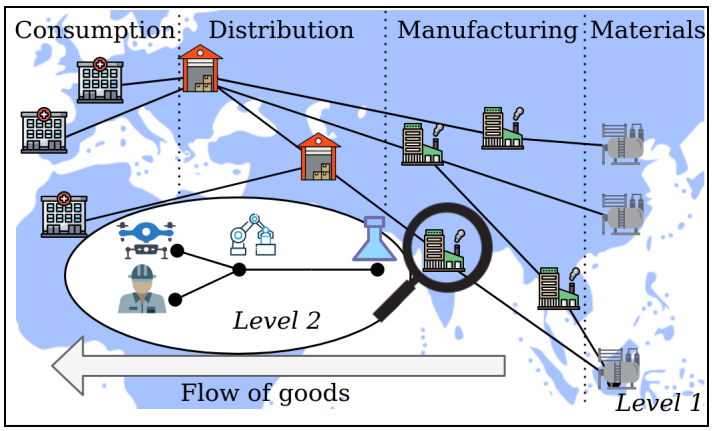

Fig. 1. Globalised pharmaceutical supply chain.

SCs are inherently *value-driven* where the precursors and final products are assets which are all potential targets of fraud. They also contain value in supporting assets e.g. machinery, vehicles, people, IT, data, geographical space, contractual agreements, social, corporate and public relationships. Therefore this *asset-rich* environment creates a *value-rich* attack surface suitable for varying forms of fraudulent deception. In general, fraud in the SC could result in integrity violations of any one of these assets [4] [14].

Threats to the SC are classified as originating *internally* from the organisation, or *externally* from the network or environment [15]. Given the wide scope of fraudulent activities, we focus and define SC fraud as *an incident of fraud in which the movement of assets between SC entities results in a deceptive transfer of value*. Fraudulent deception begins in one entity and is complete once the asset has successfully been transferred and approved by the receiving entity. The deceptive transfer of value from the victim to the deceiver occurs as a result of a SC assets transfer. This value could be taken from one or more assets. For example, the asset transferred being of lower value than agreed, or an entity's public image reduced due to substandard products. The fraud occurring across organisational boundaries increases the complexity of any subsequent investigation. Fraud that occurs internally to an organisation, such as theft of assets by an employee, is not focused on an asset transfer, and for our purposes, in this paper, it is not considered SC fraud. However, an internal employee who takes bribes to ignore a low quality product being received or distributed is classed as SC fraud. In this instance the employee is colluding with an external organisation.

Fraud should be considered during SC Risk Management

(SCRM) which allocates hard (physical) or soft (managerial) controls according to the perceived risk [1]. Therefore, fraud is *enabled* in the SC where controls have been inadequately applied or risks not sufficiently considered or prioritised [16]. The assets listed previously can be targets for controls depending upon the type of fraud which needs to be reduced.

Quality Inspection (QI) is often used to verify product integrity as it moves upstream and can be useful in detecting instances of fraud. However, *testing policies* (technique selection) are often known to the supplier and attempts to subvert them are common [17]. QI is constrained by physical SC characteristics such as the high volumes of assets, large size and geographical distribution. As such, pervasive testing is cost-ineffective. Therefore, *sampling policies* must selectively choose when and where to inspect, where *inspection resource allocation* is an on-going and key problem [18].

The cyber-physical nature of SCs brings further risks with the increase of cyber attacks, yet it also creates the potential for data-driven detection [19] [20] [21]. Downsides to these approaches focus on the availability of suitable data, particularly within dynamic environments. Further complicated by their cross-organisational and cross-jurisdictional nature, proprietarity reducing interoperability and conflicts between operation and information technologies. However, increasingly integrated SC systems may promote opportunities to mitigate these data-availability issues and allow more resource-efficient inspection. In the next section we elaborate on QI and consider a data-driven approach to promote its use for fraud mitigation in emerging integrated cyber-physical SCs.

B. Supply Chain Quality Inspection

Inspection of assets, processes and people can be found in many forms across the SC. QI is employed by both the manufacturer and consumer of a product to verify if an agreed upon standard or requirements have been met [17]. SC partners may audit each other by inspecting facilities to ensure they meet the standards agreed upon within their contractual obligations [14]. Other assets including machinery, buildings, electronics, vehicles and physical security controls may be inspected to ensure they meet health and safety standards or are operating correctly [22].

The basis of inspection requires: a *target* - an asset which is *valued* by the stakeholders whose characteristics are verified against instance specific requirements, and a corresponding *technique* - which can interface with the target and provide data to validate the requirements, which has an associated cost and accuracy. Inspection also has one or more *constraints* - mostly fixed and variable costs related to the inspection process and its impact upon the nominal SC functions.

Targeted inspection is necessary as total observation is cost inefficient while also eroding privacy and trust. The variety of different SC assets illustrate the scale of possible locations available for inspection and corresponding techniques required. Given the size and dynamic nature of SCs, the key problem is in planning when, how, and where to inspect or the *inspection resource allocation problem* [18] [17].

Approaches to manage QI resources often have statistical basis [17], as defects in products and the processes that manufacture and inspect them are considered inevitable due to the stochastic properties of the natural world [23]. Inspection can occur considering a probability distribution. Where the cost of inspection can be balanced against the probability of a defective product occurring and/or errors in testing methods [24]. Avoiding QI to save costs is known to have a detrimental effect in the longer term [25].

Yan et. al. highlight that statistical methods are thwarted by intentional human action such as defrauding a testing technique [17]. They use Belief Desire Intention (BDI) modelling as a Decision Support System (DSS) to consider when an actor may choose to defraud inspection. They take this approach further by illustrating that DSS can reduce incidences of fraud through learning intentions from QI and instigating contractual changes in response [18]. A similar relationship between the contract and QI is found in [26]. Although the authors in [27] evidence that inspection policies can influence a decision to commit fraud in cold-vaccine SCs, sometimes excessive inspection does not. While in [28] the authors illustrate that QI alone cannot prevent defrauding, as deferring payment or other incentives are necessary. From the above work it can be seen that QI can be employed to mitigate fraud in the SC, although traditional approaches are still resource constrained by physical inspection processes and should consider additional human motivated factors to be successful.

C. I4.0 Supply Chain

I4.0 SC seeks to accomplish the same goals as the traditional SC. It operates upon data-rich, integrated, autonomous and decentralised environments built upon the principles of multi-dimensional integration [29]: Horizontal inter-corporation co-operation across departments; Vertical within the factory; and End-to-end in the form of product data across the VC.

The migration from a manufacturing environment with low digital technology penetration to one which is strongly automated is a primary indicator of I4.0 maturity. Whilst the highest level of maturity can be considered complete once this digital penetration is integrated across the entire VC [29]. The authors in [10] and [30] model this evolution from the perspective of the IEC 62264 automation pyramid yet with the inclusion of cross-organisation decentralised decision making. The once linear SC model has now evolved into a nonlinear transfer of goods across a network which operates across a unified organisation. Moreover, *value* drives the dynamic nature of the SC as a result of greater horizontal and end-to-end VC integration [7]. In contrast to the SC which involves the physical movement of goods from one point of the chain to another, the VC is responsible for the creation of value at each step. Therefore as an addition to the decentralised SC model, I4.0 contains decentralised VCs or *value-networks*. Traditional SC environments, which were a linear process composed of distinct entities, is now moving to a decentralised, non-linear process where entities are integrated through digital means. This creates a fundamentally different landscape, requiring

new processes for analysing fraud which consider these value-driven structures. The data-rich I4.0 environment contains cyber-physical interfaces into all assets to accommodate integration, yet integrated approaches to inspection planning in I4.0 are generally absent from literature [5].

IV. Topology-aware Adaptive Inspection

In this section we propose *adaptive inspection of supply chains*. We propose the creation and maintenance of *SC topologies* to represent SCs and their relevant context. Based on these topologies and the key assets of value they represent, we derive optimal *inspection zones* that also account for additional constraints such as privacy and cost. We define an inspection zone as a precise fragment of a supply chain topology which will contain one or more assets. It can be generated computationally - and optimally - around assets of interest according to the value and risk of fraud associated with the assets, while also accounting for constraints such as the cost of executing the inspection. Inspection costs are contextual and can be *fixed* or *variable*. They can involve the cost of executing the technique, but also the impact of the inspection through disrupting processes and reducing trust.

Figure 2 presents the overall concept based upon the Monitor Analyse Plan Exeute-Knowledge (MAPE-K) feedback loop reference model [31]. The lowest layer is the SC, which contains the physical structure and the I4.0 data integration layer. This layer supports the topology layer that builds SC topology models, which are stored in the knowledge base. The topology models represent the structure of the SC (including its assets) and can be *monitored* for changes, reducing observability. The models contain information about actors, their assets and those assets that move between them. They also contain information about the relationships between these components such as their reachability and containment which identify the value of inspecting a particular point. The topology models are *analysed* to assess the value of different assets and to determine if and what should be inspected. To improve observation of the environment, inspection is *planned* of particular inspection zones. Finally, the inspection plans are *executed* through highlighting areas of concern in the topology layer. The topology layer then translates these locations into cyber-physical inspection locations where they are acted upon in the cyber-physical SC. The result of which updates topologies in the knowledge base to inform future inspection decisions.

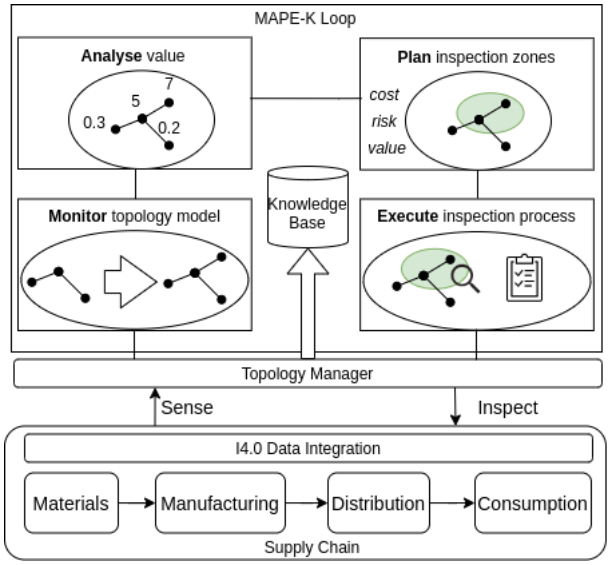

Fig. 2. Topology Aware Adaptive Inspection of Supply Chains

A. Generating Topology Models

SCs describe a typically linear process in which assets move through a sequence of processes causing a corresponding sequence of state changes. We consider them as *spatiotemporal* with the SC structure corresponding to the dimension of space and the changing state of the assets across processes representing time. Figure 3 illustrates a SC, represented as a Directed Acyclic Graph (DAG), where a manufacturing process has been chosen from the level 1 SC topology (see motivating example in fig. 1). The vertices in the DAG correspond to models of physical processes within the manufacturing process, which receive *assets* as input and will then undergo a state transformation according to one or more states of the cyber physical process For example, consider node *2.1 Warehouse* and *2.2 Milling Machine* from fig. 3. The asset in fig. 4 will change state from *packaged* to *raw* according to the process state *2.1:unloading* from *2.1 Warehouse* and then the *2.2:loading* process state from *2.2 Milling Machine* will cause the asset to move to state *processing*. The approach takes data of the physical, cyber and process structures of the supply chain and generate new topology models, which describe the combined cyber-physical SC processes in a way that represents the relationship between them such as their containment.

Formally, we define the supply chain topology as a tuple $SC = (P, E, H, \mu, F, \delta, K, \kappa)$ where: P is a set of combined cyber-physical SC processes (e.g. $\{MillingMachine, ShippingDepot\}$; E is a list of ordered relations between the processes $E \subseteq P \times P$; H is a set of process identifiers; μ is a mapping between processes and their attributes $\mu : P \rightarrow H$; F is a set of unique flags used to maintain a track of inspection outcomes (e.g., a negative, neutral or positive inspection $\{-1, 0, 1\}$); and $\delta : P \rightarrow F$ is a mapping between processes and flags. $h \in H$ is used to identify and verify the processes (such as a unique hash of the process function), to ensure the relations δ are current. $p \in P$ may be another topology representing its sub-processes or $\emptyset$ depending on the level of detail required to the model. This permits multi-level topologies. Finally K is a set of container environments (e.g. $\{MachineRoom1, MachineRoom2\}$, and κ is a mapping between process p and containers $k \in K$ to illustrate their containment.

As an asset moves through the SC processes, it will undergo a sequence of state changes which may adjust its value, although the particular order and number of states is unknown due to the dynamic nature of the smart manufacturing environment. Formally, a tuple $AST = (A, V, \sigma, C, \tau)$ where A

is a set of asset states, V is a set of value changes such that $V \subset \mathbb{R}+$, σ is a mapping between asset states and changes in value $\sigma : A \to V$, C is a set of cyber physical SC process states e.g. $\{unloading, loading, milling\}$, and τ is a mapping in which the SC process transmutes an asset from one state to another $\tau \subseteq A \times C \times A$. A subset of an asset model in the SC in fig. 3 could be represented as a Labelled Transition System (LTS) as in fig. 4. In the I4.0 context we propose that these models can be autonomously built using data available from the integration of manufacturing and supply chain systems, and assume this data is available for this purpose in the rest of this work.

B. Monitoring SC Topology Models

As greater observation reduces fraud, the goal of the inspection is to improve observability. In this stage, the generated topology models are monitored to identify significant changes. This could include the structure of the SC changing due to factories re-configuring, new suppliers entering the SC, transport routes closing, smart products changing their path as a result of changing customer needs, or machine configuration changes as a result of updates. In the SC topology given previously, the unique attributes H will be used for this comparison, typically storing a cryptographically secure hash of identifiable I4.0 data, and compared using the relevant hash function (e.g. SHA256) [32].

C. Topology Value Analysis

The SC topology models provide the *inspection surface* with a set of spatio-temporal coordinates suitable for inspection. An analysis of this inspection surface determines the *value* for inspection, which can be later balanced against the *cost*. Value analysis must be computable at varying scale to permit timely operation while considering the environment and its context. Value analysis may take many forms. We first analyse the environment's structure using degree centrality, which indicates the importance of a node according to its connections [33]. This is useful as a higher number of connections correlates to a higher level of observability of the network through observing the input and output of different processes. This approach is less intrusive than inspecting directly since it reduces the disruption and cost, and increases the value of the inspection.

The approach selects all processes within the topology that are suitably flagged according to previous inspections. $Q = \{p : p \in P \wedge \delta(p) > 0\}$ where $\delta(p)$ is given in equation 1.

$$\delta(p) = \begin{cases} -1 & \text{if } p \text{ inspection was negative} \\ 0 & \text{if } p \text{ inspection was positive} \\ 1 & \text{if } p \text{ has not been inspected} \\ 2 & \text{if } p \text{ should be prioritised for inspection} \end{cases} \tag{1}$$

Following the selection of process, centrality is calculated in the normal way for each $q \in Q$, $C_D(q)$. The value model is a tuple $VM = (X, \lambda)$, where X is a set of centrality values multiplied by corresponding contextual value $x \in X = q \cdot v$ with $v \in V$ as previously defined contextual value in the asset model. Finally $\lambda : X \times A$ maps the asset state to its combined value. The contextual value acts as a multiplier, whose sensitivity will be adjusted according to the requirements. A product with high financial value would be reflected in the context and thus scale the value accordingly. Whether the optimisation would seek a high or low value is scenario-dependent. Cases of theft could consider high value and adulteration low. In I4.0 environments such information would be available in the form of asset models (e.g. [34]). We assume the availability and usability of this data for inspection analysis.

D. Inspection Zones Planning

Once the value analysis has been computed, inspection can be planned by defining inspection zones around one or more assets according to available inspection resources. Inspection Zone Planning (IZP) involves selecting a subgraph of the SC topology according to the *value* of inspection against the cost. IZP is a combinatorial optimisation problem and, therefore, a variety of search-based solutions may be applicable. IZP could be considered as an instance of the knapsack problem [35], with the purpose of maximising the value of inspection associated with the asset state's value. This is similar to the value model (VM) within constraints of inspection cost, which correlates to the knapsacks total weight constraint. Consider the asset states $a \in A$, values x_i with costs c_i, maximum inspection cost Z. Equations 2 and 3 denote the IZP.

$$\text{Max} \sum_{i=1}^{|A|} x_i a_i \tag{2}$$

$$\text{Subject to} \sum_{i=1}^{|A|} c_i a_i \leq Z \text{ and } a \in \{0, 1\} \tag{3}$$

In order to find a solution to IZP, the cost of inspecting each location and the maximum cost allowed must be calculated from costs directly associated with the inspection process and contextually associated with the environment. The complexity and scale of these costs are out of the scope of this paper. C_a the cost of inspecting asset state a is simply the sum of the elements of all direct D_a and contextual K_a costs.

E. Executing Inspection

Inspection can be executed based on the defined processes and assets. The result of the execution will inform the next iteration of the MAPE-K loop. It can exclude places previously inspected and flag processes adjacent to those which are subverted to ensure completeness. The inspection function $\iota(a)$ returns the result of the integrity evaluation of a process and asset (positive or negative), which is added to the topology model.

V. Running Example and Discussion

In order to consider the example in Section II. Suppose some pharmaceuticals were identified as low quality through consumer complaints and one manufacturing factory was chosen for inspection.

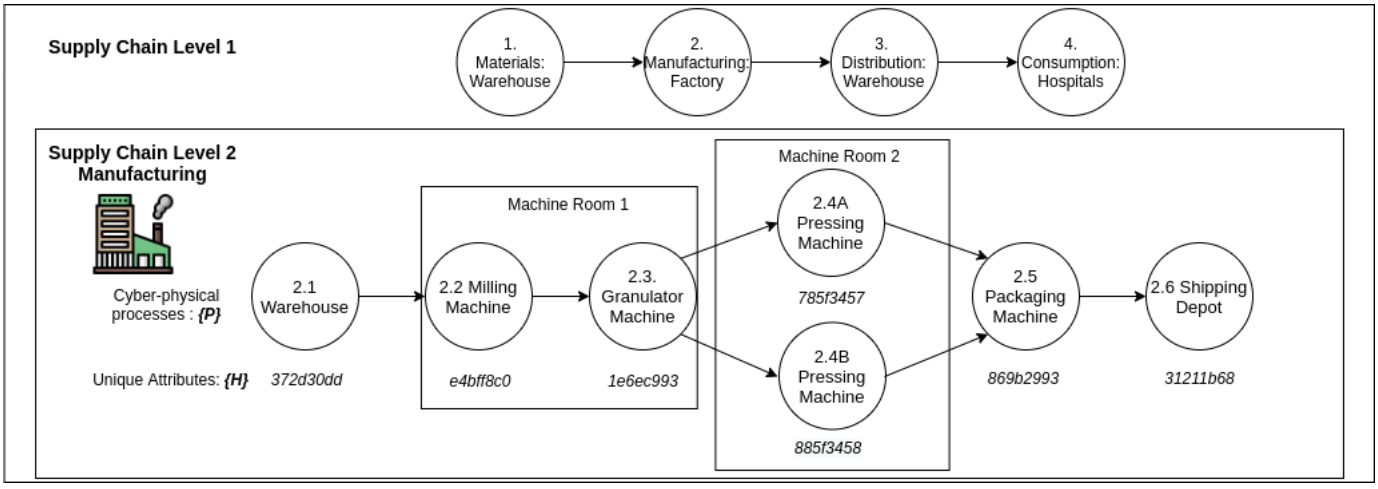

Fig. 3. A cyber-physical supply chain topology represented as a DAG. Illustrating Level 2 of a topology contained within level 1, with two further containment relationships in machine room 1 and 2.

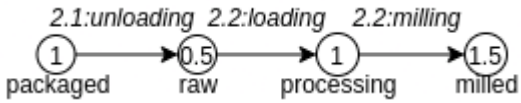

Fig. 4. A subset of an asset model represented as a LTS undergoing state changes from supply chain process with example contextual value changes

Consider monitoring a version of the SC topology from the example of the factory in fig. 3 and noticing that observability of the network is low as all flags are set to 1; likely due to a considerable change or due to no prior inspection. A value analysis is performed to determine where best to inspect. Degree centrality analysis is first used, then contextual value from the asset model is added. In this case *2.5 Packaging Machine* is reduced by 50% as it is unbranded and, therefore, not highly valued and less relevant to an adulterated chemical process. Meanwhile *2.2 Milling Machine* is increased by 20% due to high operational costs and the high negative effects of doing it incorrectly. Assume contextual costs (k_j) to 0.2 for all inspection points, and direct costs arbitrarily $0 \leq d_i \leq 1$. Table I lists the final parameters for all flags $\delta(p) = 1$ in the first iteration. Consider all points contained in *Machine Room 2* with a higher inspection cost due to its location.

TABLE I
INPUT PARAMETERS FOR STARTING ITERATION

Proc. (p)	**Centr.** (q)	**Asset** (a)	(v)	**Val.**(x)	**Cost** (c)
2.1. Wareh.	0.2	Packaged	1	0.2	0.4
2.2. Milling	0.4	Milled	1.2	0.48	0.46
2.3. Granul.	0.6	Granulated	1	0.6	0.57
2.4A Press.	0.4	Pressed	1	0.4	0.89
2.4B Press.	0.4	Pressed	1	0.4	0.89
2.5 Pack.	0.4	Packaged	0.5	0.2	0.59

Suppose the integrity of processes *2.Milling* and *3.Granulation* as subverted. We implemented a Python script which models and analyses the topology using the NetworkX library [36], and a greedy approach to solve the IZP with maximum inspection cost $Z = 1$. Table II presents the results of the five other iterations, with the an iteration number (N), costs and values for each zone, and values of the flags for the processes.

As shown in table II, *2.3 Granulation* and *2.1 Warehouse* are first chosen for inspection according to the maximum value. Inspection identifies *2.3. Granulation* as subverted and flags the adjacent nodes as priority ($\delta(p) = 2$) for the next iteration to ensure that all surrounding subverted processes are discovered. In the next iteration it identifies *2.2 Milling* also as subverted and *2.4A Pressing* and *2.4B Pressing* as clear. Up to iteration $N = 4$, the results show the identification of the subverted processes as $\delta(p) = -1$. In iteration $N = 4$ we observe the ability to adapt to the changing environment. The discovery of the subverted nodes causes the factory to reset their configurations, this has the effect of changing the unique attributes and the flags are reset to 1 in *2.2 Milling* and *2.3 Granulation*, in iteration 5 as the topology has changed. The IZP then selects *2.3 Granulation* for inspection where it is now identified as not subverted.

A. Discussion

Comparison and Performance. Adaptive Inspection for fraud is suitable, scalable and effective for the environment when compared with alternatives [17] [23]. Due to the complexity of cyber-physical environments, *topological modelling* is crucial to correctly define the inspection surface where previous works fail to account for this interplay and properly leverage the cyber domain [17] [18] [26] [27] [28]. Alternative solutions to inspection resource allocation [23] involve a statistical analysis of product sampling or inspection station placement which fail to take into account human-motivation such as our application of *value-analysis*, which is crucial for fraud. Furthermore, inspection of I4.0 environments must be adaptive due to environmental flux such as re-configuring factories. Considering inspection as a search problem, comparative solutions to search for a node within the graph, (e.g. a binary search) may

TABLE II
ADAPTIVE INSPECTION OF THE RUNNING EXAMPLE ILLUSTRATING 5 ITERATIONS OF THE MAPE LOOP

	Inspection Zone Planning			Flags					
N	**Zones**	**Cost**	**Value**	**2.1Warehouse**	**2.2Milling**	**2.3Granulation**	**2.4APressing**	**2.4BPressing**	**2.5Packaging**
1	{2.3 Gran., 2.1 Wareh.}	0.97	0.67	0	2	-1	2	2	1
2	{2.2 Milling}	0.46	0.48	0	-1	-1	2	2	1
3	{2.4A Pressing}	0.89	0.4	0	-1	-1	0	2	1
4	{2.4B Pressing}	0.89	0.4	0	-1	-1	0	0	1
5	{2.3 Granulation}	0.57	0.6	0	1	0	0	0	1

-1 = Negative inspection, 0 = Positive inspection, 1=Not yet inspected, 2 = Prioritised for inspection

need to be restarted in case of changes. Therefore, inspecting dynamic I4.0 environments for fraud in a non-adaptive way is costly with the potential of not finding a solution. Given the data-intensive nature of adaptive inspection it will be essential to implement the system while being mindful of any excess resource overhead.

Value vs. Values. SCs are driven by the value of assets, products and the chain of value producing businesses services. Key to this approach is the application of value (such as money) as a means for identifying human motivated activities such as fraud. The high complexity of these values pose challenges to their collection and analysis. Therefore, developing and evaluating ways to identify, analyse and compare contextual value within smart manufacturing environments is crucial to this ongoing work. However, this can be at odds with supporting *human values*, that aim to ensure that systems are designed, developed, and deployed responsibly, reflecting the values of the stakeholders, its users, and society. Ignoring human values in SCs can have negative economic impact, cause reputation damage, and cause systems to be developed with inherent bias [37]. Therefore, a key challenge is to ensure that SCs build in, maintain and guarantee the values of their stakeholders. Additional challenges arise when SC stakeholders have divergent values, or disparities that give rise to adversarial behaviours that enable fraud [2]. The SC in the motivating example stretches across multiple jurisdictions and continents with clear cultural and linguistic differences. If inspection is to support the needs of all stakeholders and to be a benefit and not a hinderence to the SC integrity, then it must consider human values. It is necessary to ensure that base measurements of value also consider human values, and that these metrics are complimentary and not contradictory. Technical solutions must be developed to identify, operationalise and negotiate human values.

Local and Global. SCs may be considered as systems of systems, in which each system is capable of operating independently of the wider chain and having independent goals. Inconsistencies between local and global goals can give rise to conflict between systems. Identifying and managing conflicts between perspectives is a key challenge to ensure that inspection supports the needs of all stakeholders. The adaptive inspection process will differ depending upon whether it should support the goals of one SC actor (local) or the entire SC (global). This will introduce issues related to decentralisation of the adaptive feedback loop, which is an ongoing challenge in this field [38]. As shown in our pharmaceutical example (see Section II), the inspection process supports the distributor and consumer, but less so the manufacturer. To achieve decentralised adaptive inspection, data availability needs to be further stressed, as components of the system will likely be operating in different geographical spaces and timezones, and with a different perspective of the data. Coupled with the volatility and scale associated with data in smart manufacturing environments, ensuring data synchronisation will be crucial.

Forensic Readiness. Forensic readiness (FR) refers to the ability of an organisation to collect and store digital data, proactively, in order to maximise its use while minimising costs of future investigations [39]. In case an inspection discovers serious problems that require escalation to full internal or external forensic investigation, relevant data may not be admissible in a court of law due to tampering or improper handling (e.g., a broken chain of custody). Without FR, data may not be available at the time of an investigation due to its volatility [40], which may mislead to wrong conclusions. In the pharmaceutical example, once a subverted node is discovered, the incriminating data about that node should be forensically acquired and stored. However, the smart-factory may wish to resume operations quickly to prevent financial losses. Even with data being available, it can be arduous to identify relevant data among the large amount of data produced by a SC. The first challenge is the resource intensive nature of collecting and storing forensically sound data given the large scale and complexity of SCs. This is a target for abuse given its potential for privacy invasion. Further challenges lie with the interoperability of these systems. Systems will need to negotiate and manage forensic ready data formats and authorisation capabilities. Novel protocols and schemas will need to be developed or adapted to ensure seamless and transparent integration between forensic ready systems, in order to ensure standards are maintained within the SC.

VI. CONCLUSION AND FUTURE WORK

In this paper we proposed adaptive inspection to provide more dynamic observation of I4.0 SCs for mitigating fraud. We further suggested that inspection zones can provide a building block for more targeted and optimised adaptive inspection. We illustrated the approach through a Globalised Pharmaceutical example and derived an agenda of research challenges. In future work we will evaluate the approach in real case studies in terms of its performance, cost and effectiveness under

varying SC dynamics. We also plan to expand the work to support the identified challenges in particular support for human values and inconsistencies between local and global goals in complex SCs.

ACKNOWLEDGEMENT

This work was supported, in part, by Science Foundation Ireland grants 16/RC/3918, 13/RC/2094_P2 and 16/SP/3804 and EPSRC grants EP/R013144/1 and EP/S036091/1.

REFERENCES

[1] S. M. Van Ruth, P. A. Luning, I. C. Silvis, Y. Yang, and W. Huisman, "Differences in fraud vulnerability in various food supply chains and their tiers," *Food Control*, vol. 84, pp. 375 – 381, 2018.

[2] S. F. Halabi and L. O. Gostin, "Chapter 5 - falsified and substandard medicines in globalized pharmaceutical supply chains: Toward actionable solutions," in *Food and Drug Regulation in an Era of Globalized Markets*, S. F. Halabi, Ed. San Diego: Academic Press, 2015, pp. 51 – 61.

[3] D. A. Bodner, "Mitigating counterfeit part intrusions with enterprise simulation," *Procedia Computer Science*, vol. 61, pp. 233 – 239, 2015, complex Adaptive Systems San Jose, CA November 2-4, 2015.

[4] L. Manning, "Food fraud: policy and food chain," *Current Opinion in Food Science*, vol. 10, pp. 16 – 21, 2016, innovation in food science • Foodomics technologies.

[5] M. Rezaei-Malek, M. Mohammadi, J.-Y. Dantan, A. Siadat, and R. Tavakkoli-Moghaddam, "A review on optimisation of part quality inspection planning in a multi-stage manufacturing system," *International Journal of Production Research*, vol. 57, no. 15-16, pp. 4880–4897, 2019.

[6] E. Hofmann and M. Rüsch, "Industry 4.0 and the current status as well as future prospects on logistics," *Computers in Industry*, vol. 89, pp. 23–34, Aug. 2017.

[7] D. Buhr, *Social innovation policy for Industry 4.0*.

[8] M. Hermann, T. Pentek, and B. Otto, "Design principles for industrie 4.0 scenarios," in *2016 49th Hawaii International Conference on System Sciences (HICSS)*, 2016, pp. 3928–3937.

[9] H. Lasi, P. Fettke, H.-G. Kemper, T. Feld, and M. Hoffmann, "Industry 4.0," *Business & Information Systems Engineering*, vol. 6, no. 4, pp. 239–242, Aug. 2014.

[10] S. Plaga, N. Wiedermann, S. D. Anton, S. Tatschner, H. Schotten, and T. Newe, "Securing future decentralised industrial iot infrastructures: Challenges and free open source solutions," *Future Generation Computer Systems*, vol. 93, pp. 596–608, 2019.

[11] M. Salehie, L. Pasquale, I. Omoronyia, R. Ali, and B. Nuseibeh, "Requirements-driven adaptive security: Protecting variable assets at runtime," in *2012 20th IEEE international requirements engineering conference (RE)*. IEEE, 2012, pp. 111–120.

[12] F. Peters, S. Hanvey, S. Veluru, A. E.-d. Mady, M. Boubekeur, and B. Nuseibeh, "Generating privacy zones in smart cities," in *2018 IEEE International Smart Cities Conference (ISC2)*. IEEE, 2018, pp. 1–8.

[13] U. Arnold, J. Neubauer, and T. Schoenherr, "Explicating factors for companies' inclination towards corruption in operations and supply chain management: An exploratory study in germany," *International Journal of Production Economics*, vol. 138, no. 1, pp. 136–147, 2012.

[14] G. Van Drunen, M. O'connell, M. F. Hansen, S. Tavares, and K. S. Waldrop, *Supply Chain Fraud: An holistic approach to prevention, detection and response*. [Online]. Available: https://assets.kpmg/content/dam/kpmg/be/pdf/Markets/supply-chain-fraud.pdf

[15] G. E. Smith, K. J. Watson, W. H. Baker, and J. A. P. II, "A critical balance: collaboration and security in the it-enabled supply chain," *International Journal of Production Research*, vol. 45, no. 11, pp. 2595–2613, 2007.

[16] E. Mu and J. Carroll, "Development of a fraud risk decision model for prioritizing fraud risk cases in manufacturing firms," *International Journal of Production Economics*, vol. 173, pp. 30 – 42, 2016.

[17] J. Yan, X. Li, S. X. Sun, Y. Shi, and H. Wang, "A bdi modeling approach for decision support in supply chain quality inspection," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 50, no. 3, pp. 884–898, 2020.

[18] J. Yan, X. Li, Y. Shi, S. Sun, and H. Wang, "The effect of intention analysis-based fraud detection systems in repeated supply chain quality inspection: A context of learning and contract," *Information Management*, vol. 57, no. 3, p. 103177, 2020.

[19] R. Triepels, H. Daniels, and A. Feelders, "Data-driven fraud detection in international shipping," *Expert Systems with Applications*, vol. 99, pp. 193 – 202, 2018.

[20] G. Hoberg and C. Lewis, "Do fraudulent firms produce abnormal disclosure?" *Journal of Corporate Finance*, vol. 43, pp. 58 – 85, 2017.

[21] F. Xiong, L. Chapple, and H. Yin, "The use of social media to detect corporate fraud: A case study approach," *Business Horizons*, vol. 61, no. 4, pp. 623 – 633, 2018.

[22] A. Rachman and R. C. Ratnayake, "An ontology-based approach for developing offshore and onshore process equipment inspection knowledge base," in *International Conference on Offshore Mechanics and Arctic Engineering*, vol. 58783. American Society of Mechanical Engineers, 2019, p. V003T02A084.

[23] D. N. Chorafas, "Fundamentals of statistical quality inspection," in *Quality Control Applications*. Springer, 2013, pp. 235–255.

[24] M. Khan, M. Y. Jaber, and A.-R. Ahmad, "An integrated supply chain model with errors in quality inspection and learning in production," *Omega*, vol. 42, no. 1, pp. 16–24, 2014.

[25] H. Hu, Q. Wu, Z. Zhang, and S. Han, "Effect of the manufacturer quality inspection policy on the supply chain decision-making and profits." *Advances in Production Engineering & Management*, vol. 14, no. 4, 2019.

[26] Y. Zhang and Y. Zhao, "Analysis of the third party inspection strategy under asymmetric quality cost information," in *2012 International Conference on Systems and Informatics (ICSAI2012)*. IEEE, 2012, pp. 1281–1286.

[27] Q. Lin, Q. Zhao, and B. Lev, "Cold chain transportation decision in the vaccine supply chain," *European Journal of Operational Research*, vol. 283, no. 1, pp. 182–195, 2020.

[28] V. Babich and C. S. Tang, "Managing opportunistic supplier product adulteration: Deferred payments, inspection, and combined mechanisms," *Manufacturing & Service Operations Management*, vol. 14, no. 2, pp. 301–314, 2012.

[29] E. Gökalp, U. Şener, and P. E. Eren, "Development of an assessment model for industry 4.0: industry 4.0-mm," in *International Conference on Software Process Improvement and Capability Determination*. Springer, 2017, pp. 128–142.

[30] M. Brettel, N. Friederichsen, M. A. Keller, and M. Rosenberg, "How Virtualization, Decentralization and Network Building Change the Manufacturing Landscape: An Industry 4.0 Perspective," 2014.

[31] J. O. Kephart and D. M. Chess, "The vision of autonomic computing," *Computer*, vol. 36, no. 1, pp. 41–50, 2003.

[32] D. Rachmawati, J. Tarigan, and A. Ginting, "A comparative study of message digest 5 (md5) and sha256 algorithm," in *Journal of Physics: Conference Series*, vol. 978, no. 1. IOP Publishing, 2018, p. 012116.

[33] M. J. Alenazi and J. P. Sterbenz, "Comprehensive comparison and accuracy of graph metrics in predicting network resilience," in *2015 11th International Conference on the Design of Reliable Communication Networks (DRCN)*. IEEE, 2015, pp. 157–164.

[34] F. Patzer, F. Volz, T. Usländer, I. Blöcher, and J. Beyerer, "The industrie 4.0 asset administration shell as information source for security analysis," in *2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, 2019, pp. 420–427.

[35] H. M. Salkin and C. A. De Kluyver, "The knapsack problem: a survey," *Naval Research Logistics Quarterly*, vol. 22, no. 1, pp. 127–144, 1975.

[36] A. Hagberg, P. Swart, and D. S Chult, "Exploring network structure, dynamics, and function using networkx," Los Alamos National Lab.(LANL), Los Alamos, NM (United States), Tech. Rep., 2008.

[37] J. Whittle, M. A. Ferrario, W. Simm, and W. Hussain, "A case for human values in software engineering," *IEEE Software*, 2019.

[38] D. Weyns, "Software engineering of self-adaptive systems: an organised tour and future challenges," *Chapter in Handbook of Software Engineering*, 2017.

[39] R. Rowlingson, "A ten step process for forensic readiness," *International Journal of Digital Evidence*, vol. 2, no. 3, pp. 1–28, 2004.

[40] F. Alrimawi, L. Pasquale, and B. Nuseibeh, "Software Engineering Challenges For Investigating Cyber-Physical Incidents," in *Proceedings of the 3rd International Workshop on Software Engineering for Smart Cyber-Physical Systems*. IEEE Press, 2017, pp. 34–40.