Article

Provisioning Cybersecurity in ICT Complex Supply Chains: An Overview, Key Issues and a Relevant Architecture

Xavi Masip-Bruin[1,*], Eva Marín-Tordera[1], José Ruiz[2],Admela Jukan[3], Panagiotis Trakadas[4], Ales Cernivec[5], Antonio Lioy[6], Diego López[7], Henrique Santos[8], Antonis Gonos[9], Ana Silva[10], José Soriano[11] , and Grigorios Kalogiannis [12]

[1] Universitat Politècnica de Catalunya, CRAAX-UPC, Spain; xmasip@ac.upc.edu; eva@ac.upc.edu
[2] ATOS Research and Innovation, Spain; josefrancisco.ruiz@atos.net
[3] Technische Universität Braunschweig, Germany; a.jukan@tu-bs.de
[4] Sinelixis S.A., Greece, ptrak@synelixis.com
[5] XLAB d.o.o., Slovenia; ales.cernivec@xlab.si
[6] Politecnico di Torino, Italy; lioy@polito.it
[7] Telefónica Investigación y Desarrollo, Spain; diego.r.lopez@telefonica.com
[8] Centro ALGORITMI ,Universidade do Minho, Potugal; hsantos@dsi.uminho.pt
[9] Optimum S.A. Information Technology, Greece; agonos@optimum.gr
[10] Sonae MC Serviços Partilhados S.A., Portugal; amsilva@sonaemc.com
[11] Capgemini Engineering, Spain, jose.soriano@altran.com
[12] Sphynx Technology Solutions AG, Switzerland; g.kalogiannis@sphynx.ch

* Correspondence: xmasip@ac.upc.edu

Abstract: The specific demands inherent to supply chains built upon large IoT systems, make a must the design of a coordinated framework for cyber resilience provisioning intended to guaranteeing trusted supply chains of ICT systems, built upon distributed, dynamic, potentially insecure and heterogeneous ICT infrastructures. As such, the proposed solution is envisioned to deal with the whole supply chain system components, from the IoT ecosystem to the infrastructure connecting them, addressing security and privacy functionalities related to risks and vulnerabilities management, accountability and mitigation strategies as well as security metrics and evidence-based security assurance. In this paper we present FISHY, as a preliminary designed architecture, designed to orchestrate both existing and beyond state-of-the-art security appliances in composed ICT scenarios and also leveraging capabilities of programmable network and IT infrastructure through seamless orchestration and instantiation of novel security services, both in real-time and proactively. The paper also includes a thorough business analysis to go far beyond the technical benefits of a potential FISHY adoption as well as three real-world use cases where to strongly support the envisioned benefits of a FISHY adoption.

Keywords: Cybersecurity; supply chains; IoT systems; systems integration; real scenarios analysis

1. Introducing the Scenario

The unstoppable evolution of ICT systems, with innovative technologies and business models, is driving a massive digital transformation and the Industry 4.0 revolution. At the same time, the more dependable society on ICT systems, the more critical the effects of even minor ICT infrastructure disruption. Today, the resilience of ICT systems is premium, and every ICT system is expected to implement at least a set of basic mechanisms to prevent, resist, and recover from any type of disruption in a timely manner, thus minimizing the impact on service quality and user experience. Particularly in the ICT supply chains, the ICT implementation of physical supply chains, serving multiple actors in finance, manufacturing, healthcare and many other sectors, not only individual parts of the supply chain need to be secured and reliably provisioned, but also the end-to-end process of securing the ICT supply chain. In real words, however, and according to an IBM/Ponemon study, 77% of organizations which individually or jointly participate in a supply chain process, do not even have an incident response plan. The National Cybersecurity Alliance found that 60% of SMEs would be out of business within six months of being hit by a cyber-attack [1]. On the other hand, the concept of cyber resilience is expected to become the norm, and one of the key measures of an ICT system's ability to continue its operations in the event of a cyber-attack or incident. According to the US National Institute for Standards and Technology (NIST) cyber resilience is defined as *"the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that include cyber resources."* [2]. Therefore, it is an imperative today to achieving cyber resilience of any ICT system, which is particularly a challenge in presence of disruptions, whether due to malicious security attacks or due to unreliable hardware and software system components and their implementations. Furthermore, making the entire ICT supply chain as secure and reliable as the physical supply chain is even more of challenge, especially due to the consumers of physical supply chain services are the same as the one consuming ICT supply chain, with the same expectation on service quality.

1.1. Background

In practice, an efficient resilience strategy would ideally leverage three main components: i) continuous availability, enabled by both the deployment of strategies to guarantee an "always-on" customer experience and the required protection in front of disruptions; ii) IT workload mobility, permitted by the deployment of strategies facilitating traffic offloading and resource migration in a distributed computing environment, including edge and cloud computing; and iii) multi-cloud agility (including also hybrid clouds, and coordinated edge-cloud) to determine the optimal set of resources best matching the expected level of resilience for each application. These three components are driving the deployment of the corresponding policies to providing security, trust, and performance guarantees, coupled with efficient network and compute infrastructure management strategies to optimize resources allocation, self-healing, and dynamic reconfiguration of ICT resources. Moreover, it is not the integration of these policies and strategies that must be pursued, but their effective coordination in complex multi-stakeholder ICT infrastructure scenarios. To this end, coordinated methods are also needed to forecast and accurately estimate vulnerabilities and risks potentially impacting on the performance. In turn, these forecasts can be used to assess potential risk for security and privacy and the related accountability and mitigation strategies, as well as the solutions to operate resilient services on top of potentially unreliable infrastructure components. It is in fact a major open challenge to providing these properties end-to-end, i.e., and across the entire ICT supply chain.

A further challenge to be addressed in the context of cyber resilience is its strong link to cybersecurity. Cybersecurity is one of the greatest challenges of our era. In May 2017, WannaCry malware cyberattack infected more than 200,000 computers across 150 countries, with total damages estimated to hundreds of millions of Euros [3]. During the same year, more than 26% of US healthcare consumers have experienced a breach of their healthcare data, which included their Social Security number, contact information, electronic medical record or health insurance ID [4]. This is hugely reflected and significantly amplified in the supply chain realm, among several other factors, because of the potential of the so-called domino effect. According to [5], there were reports of a worm "Stuxnet" that reportedly infiltrated Siemens industrial control software and later impacted operation of an Iranian nuclear plant through ICT supply chain. Also, in [6], it was reported that components of Boing airliner were failing due to glitches in Japanese supply chain production that affected globally airports and grounded airliners in India, Chile and United States. In [7], the authors reported from their work in an EU project, that the major crimes encountered by supply chain stakeholders in Europe were theft in transit (23 %), data theft/cybercrime (11 %), bogus companies (10 %), and insider fraud (10 %). Also, other crimes were reported including, smuggling (9 %), counterfeiting (9 %), and terrorism (6 %). Less frequent in the past, but possibly a bigger threat in the future were also environmental crimes in the supply chain [8].

Finally, according to appknox [9], the number of attacks in 2019 has grown notably when compared to previous years. And even worse, the same study reports that "*…by the year 2020, the costs related to damage caused by cybersecurity breaches may reach $5 trillion and that is why it becomes essential to ensure that your business' infrastructure is up-to-date and ready to ward off cybercrimes*".

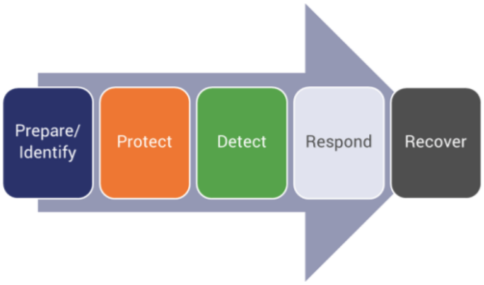

Figure 1.1. Five pillars for security evaluation

These examples illustrate that cyberattacks affect the whole spectrum of services and application domains simultaneously, and do not anymore distinguish between e-health and social media services, or industrial IoT and telecom operator networking devices, when choosing their targets. This alone establishes a strong interlink between cyber resilience and cybersecurity. Cyber resilience while relying on cybersecurity also assumes that not all parts of the system can be cybersecured, not only for economic reasons but also for reasons of usability and scalability. Hence, establishing the proper link between cyber resilience and the fundamental pillars of cybersecurity is another challenge. To this end, a proper evaluation of the cybersecurity process is needed. For instance, Symantec proposes a five-pillar approach to building the cybersecurity part of a cyber resilience plan (Figure 1.1).

Today, governments, enterprises and individuals are systematically and collectively outpaced in managing their cybersecurity systems and appliances, both by external attackers, internal threats and fundamentally unreliable and unsecured components of ICT systems. The threat is not just any more basic of sensitive information being stolen, or a website being deactivated, but a plethora of quiet and unforeseeable threats, where attackers creep in and can change systems' behaviour and network configuration at will [10]. These attacks are polymorphic in nature and sophisticated, using previously unseen custom code, able to communicate with external command and control entities to update their functionality or even implement themselves entirely from code fragments that they intelligently harvest from benign programs, scripts and software blocks already present in the cybersecurity system in place [11].

1.2. Challenges

Due to the dynamicity and sophistication of the current cybersecurity and privacy threats, security administrators and IT operators must face the following five unprecedented challenges when trying to make their system resilient.

Challenge 1: Need for end-to-end solutions for vulnerabilities and risks management:

With around 350,000 new malware programs appearing every day [12] and 88% of respondents [14] from medium-size companies replying that they receive up to 500 severe/critical alerts per day, it is evident that only a limited percentage (~1%) of the critical threats are analysed, which indicates *the lack of effective methods to characterize, detect, classify, forecast, and estimate threats, risks, vulnerabilities and suspicious activities.* On one hand, the challenge is not just detecting the vulnerability itself, but rather building an innovative solution to manage the whole vulnerabilities lifecycle, including the characteristics mentioned above, and the vulnerabilities propagation within the entire end-to-end supply chain too. On the other hand, *cybersecurity and privacy risks must also be accurately estimated within the entire supply chain* to meet performance expectations through an appropriate data sharing mechanism [13], as well as to enable dynamic updates through real-time awareness of ICT systems' actual states

Challenge 2: Lack of evidence-based metrics for security assurance and trust guarantees

Security and trust assurance should not be only inferred from an observed absence of security incidents: this observation may be an indication of the absence of attacks during the monitored period or the incapacity of the system to detect attacks. Similarly, security assurance must not only leverage on trust, but on evidences supporting specific security claims. However, there is a *lack of effective metrics to characterize composed ICT systems performance with regards to cybersecurity and privacy, thus making it difficult to provide the certification of complex systems*. Just like physical goods require metrics to distinguish between high quality goods and low-quality goods (e.g., cotton, wood, or a car), also ICT supply chain requires effective metrics, or else one cannot distinguish with highly-secure and low-security parts in the supply chain. Consequently, it is necessary to define both the security claims and the set of metrics used to characterise these claims and choose the proper evidence for each specific claim. In the context of certification, the former can be aligned with the objectives within the considered scope and target of the certification, and the latter can provide the necessary certification auditable evidence needed to verify the (continuous, where needed) compliance with the desired objectives. Said evidence and metrics must be identified at early stages of the ICT system design, towards a security and trust by design approach that optimizes the obtained results while minimizing the costs, while also considering the relevant certification and regulatory requirements of each of the covered domains to ensure that the intricacies (both in terms of objectives as well as associated controls and needed evidence) are comprehensively covered.

Challenge 3: Cumbersome coordination in multi-actor and multi-vendor supply chains of ICT systems

Security analytics, operations technologies and mechanisms are characterized by complexity as organizations are dealing with 10 to 25 different technologies [15] and involve IT administrators, network architects, software developers and several other roles within different contexts. Their interaction is complex and encompasses organizational structures as well as supply ICT chain process to design, construct, manage and protect the ICT supply chain. Given such a heterogeneous and complex cybersecurity ecosystem, *the process of coordination and orchestrated management of security appliances to provide trusted supply chains, as well as acquisition and configuration of new tools by the network administrators and IT operators becomes a challenging endeavour*. One of the daunting demanding challenges is reflected in *security policies that are often specified by people different from software developers* actually implementing them, which *leads to misconfigurations and improper response to threats and attacks, mainly due to the diversity of development contexts, multi-vendor security controls, and technology maturity levels*. Gartner estimates that 70% to 99% of data breaches result not from external, concerted attacks, but from misconfiguration (human error, software update or technical malfunction) of the affected IT systems [16]. Also, in an entire supply chain scenario, there is no a single user controlling the whole system, *thus lacking strict identity management and accountability mechanisms*

Challenge 4: Static cybersecurity networked configurations and dynamic systems audit

Even when a security policy is successfully developed and implemented, the security systems in use are rather static with respect to highly dynamic threat prevention and mitigation techniques needed. In most of the cases, *neither the network elements nor the security appliances support a reconfiguration framework to meet the pace of highly dynamically changing nature of cyber threats*. The ease of attacking an ICT supply chain is largely due to network. The network actually amplifies the security threat in the supply chain significantly. While newly proposed concepts of Network Function Virtualization (NFV) and previously of Software Defined Networking (SDN) have opened up the window of opportunity to dynamically control the network, this has neither be used in connection with dynamic security policy enforcement nor for an effective protection against cyber threats, quite the contrary [17]. *The network challenge is further exacerbated considering the influx of the* *resource constrained nature of IoT devices and the myriad of potentially insecure devices to be all interconnected in a typically complex ICT system today. This requires innovative methods to developing resilient systems on top of a myriad of fundamentally insecure components and novel tools to better audit the different systems and interconnected components*

Challenge 5: Unlikely wide adoption of integrated cybersecurity solutions for composed ICT systems

While several commercial cybersecurity solutions exist offering integrated solutions to network and IT administrators, integrated solutions in general remain beneficial for specialized environments only (military, governments, large financial player). In the commercial sector, *integrated approaches are proven to be complex, and requiring large operational expenses, along with a high learning curve for human administrators or complex integrated systems.* Indeed, training security administrators how to orchestrate and implement security services on new systems in a highly specialized platform solution takes significant time and financial effort. In fact, *these solutions are not designed to meet the requirements of fast evolving, large-scale heterogeneous systems as in typical supply chains built on top of complex ICT systems, or to facilitate the proper data sharing and performance metrics benchmarking for ICT systems among different stakeholders*. Thus, new approaches are needed to facilitate a coordinated rather than integrated deployment of cybersecurity solutions considering the complexity of supply chains putting together composed ICT systems from different stakeholders, handled by human resources with different levels of skills in ICT management.

1.3. Contributions

Taking into consideration the challenges identified above, in this paper an architecture for cybersecurity provisioning in supply chains built upon complex ICT systems is proposed. More specifically, the contributions of this work are as follows:

- A thorough literature review on the main relevant areas is given, including information security assessment, policy-based systems, trust monitoring, authentication, and threat anomaly detection among others.
- The presentation of an innovative architecture, referred to as FISHY, for providing cybersecurity guarantees in supply chains of complex ICT systems consisting of: i) innovative integrated services capable of intent-based orchestration of security appliances through a well-defined toolset; ii) an evidence-based security assurance and certification methodology; iii) a multi-party supply chain verification and forecasting system based on Distributed Ledger Technology (DLT), and; iv) a fully integrated, tested and demonstrated platform on three verifiable supply chain systems built upon three real industrial pilots.
- Discussion on several business aspects, aiming at emphasizing the impact of the proposed architecture, as well as its potential adoption by key stakeholders.
- Three real industrial pilots are presented, highlighting the benefits brought in by a possible deployment of the proposed architecture.

1.4. Outline

This paper is organized as follows. Section 2 revisits the literature in the closely related research areas this paper focuses on. Then, Section 3 introduces the proposed FISHY architecture along with its functional blocks. Section 4 describes the business scenario, emphasizing the involved stakeholders and potential market opportunities, as well as the factors that may hinder a wide adoption of the proposed solution. Next, Section 5 presents three potential use cases as potential scenarios for a FISHY deployment. Finally, Section 6 concludes the paper.

2. Review of the State-of-the-art

This section revisits current literature in fields closely linked to the proposed FISHY architecture.

2.1. Information Security Assessment

Information Security Assessment (or Cybersecurity Assessment) can be defined in different ways, according to the standards already available (mainly from ISO/IEC, CEN, and NIST). Some of them are focused on the devices' security requirements accomplishment, others on the environment's threat levels, and others on the effectiveness of the security control in place [18]. Those standards also help to characterize the assessment process, usually based on the technical analysis of the components (including vulnerability analysis), working tests (typically taking the component as a block-box), or just surveying functioning perception by operators [19]. Whatever method is used, a key central issue is always the quality of the metrics used (frequently constrained by observability). In fact, the security metrics problem has been researched along the last years and, despite some solutions for particular cases (like smart grids, or nuclear plants), there are no recognized generic model satisfying most implementations, particularly those where system diversity is the main characteristic, like in the IoT paradigm [20], [21], [22].

A good metric should have some fundamental properties (objective, measurable, attainable, repeatable, accurate, and time-dependent), and it can be linked to several system dimensions, like networks, software, users, and policies, eventually with a more fine-grained sub-classification scheme [23], [24]. There are relevant scientific work addressing the metric definition problem, from ontological classification schemes to models supporting metrics definition, like the MDGSM (Method for Designing Good Security Metrics) [23]. The subject was also targeted by well recognized standards (e.g., ISO 27004, and NIST SP 800-53), which normally include application guides [25], [26]. Finally, there are some attempts to use more complex multi-criteria solutions that explore relations and dependencies between different metrics, aiming to improve the decision-making process [27]. However, none of the aforementioned works can support an efficient set of metrics addressing the complexity and diversity present in IoT-based solutions.

2.2. Policy-based Systems

Networks are traditionally configured (and reconfigured) manually, or with a very limited support from automatic tools. The rapid adoption of new IoT technologies has furthermore increased the ever-growing complexity and heterogeneity of modern IT infrastructures. Having a fully protected and efficient network in this scenario is thus becoming increasingly difficult, requiring the use of automatic tools to handle it in a timely and error-free manner.

To ease the pain of configuring a network, the introduction of systems that can automatically refine high-level security policies into configurations or lower-level policies has been already proposed in the current scientific literature. There exist very few papers on this subject [28], [29], [30] and the adoption of an automatic refinement work-flow in production systems has been scarce to non-existent for several reasons.

First, automatically translating high-level policies to lower-level policies or configurations is hard and requires a significant level of intelligence, unless the policies are very simple, or the landscape has a trivial architecture. Intrusion Prevention Systems (IPS), such as Snort [31] and Suricata [32], can be though as a form of simplified policy refinement systems, since they can be effectively configured to automatically use different reaction policies when an attack has been detected. Despite the adoption of IPS solutions in production environments, their "refinement engine" limit their usability only in situations when the countermeasure is nearly trivial (e.g. drop all the suspected attacker packets).

Second, translating a policy is not enough in complex scenarios. Once a set of security configurations has been generated, it is also important to actually deploy them in the right order since a wrong one can temporary create an insecure state where the network security level has been lowered. Virtually no policy refinement system as of today offers this capability

2.3. Trust Monitoring

Traditional strong integrity verifications of an IT infrastructure nodes are performed on physical nodes via the remote attestation procedure, which was standardized by the Trusted Computing Group [33] as a method to provide hardware-based integrity verification of an IT system via an ad-hoc chip named the TPM (Trusted Platform Module). This allows to continuously check the status of the software, services and configurations deployed on a host [34], [35]. This approach is, however, not necessarily ideal in heavily virtualized environments, where most of the jobs are done via virtual machines and especially containers (lightweight virtual machines). Using this approach, in fact, the virtual machines can only be attested at deployment time and not during their run-time.

While remote attestation allows to verify only the integrity of the software, it cannot be used to check the traffic that is sent through the network. The classic way to detect unauthorized changes to the traffic flows is to make use of secure channels via specific protocols such as TLS [36] or IPsec [37]. All these technologies allow to ensure the confidentiality of a transmission (via encryption) or its authenticity/integrity (via digital signatures or MACs), however, they do not allow to verify if a packet was effectively sent, received or traversed all the nodes that it was supposed to go through.

2.4. Authentication and Authorization / Security Requirement Management

It is widely accepted that the characteristics inherent to devices located at the edge of the network (such as the IoT devices) are making hard to provide security guarantees to their users, thus potentially hindering the large adoption of such devices in order to support innovative services. Aspects such as devices mobility, heterogeneity and low computing capacities may add serious risks to all scenarios where these devices are to be deployed. Thus, any system, platform or solution leveraging IoT devices to run services must provide several security requirements for granted, as those listed below [38]:

- authentication. Edge devices must be authenticated to both cloud (upper layer) and other edge devices (lower layer), allowing only the authorized nodes to communicate and get data. One of the main challenges here is to authenticate constrained IoT devices to network nodes.
- secure data sharing and data aggregation. Data sharing between edge-to-cloud must be encrypted, and data aggregation in intermediate layers must be similarly managed. However, handling data sharing and aggregation in a distributed way demands for a novel security management approach to be designed.
- secure service discovery. In order to provide services only to authorized users, services must be discovered and delivered in a secure manner, intended to avoid fake users and fake nodes.
- malicious nodes detection. Distributed nodes are vulnerable to external and internal attacks. Hence, a mechanism is needed to detect malicious nodes.
- secure virtualization. Nodes must provide a secure virtualization environment, to avoid malicious virtual machines, virtualization attacks, and prevent an attacker to take control over either the hardware or the operating system to launch attacks.

All these requirements must be met in a highly heterogeneous environment, where multiple nodes (IoT devices) are continuously joining and leaving.

2.5. Threat and Anomaly detection

Automatic detection of traffic anomalies and network cyber-attacks is not a novelty. Intrusion Detection Systems (IDS) such as Snort, Bro [39] and Suricata are frequently used in production IT infrastructures. They usually detect threats by looking at specific patterns in the traffic using advanced pattern matching rules. IDS systems are not trained but configured by experts with ad-hoc pattern matching expressions, thus limiting their effective usage for at least two reasons. On one hand, writing detection rules for new attacks requires a significant amount of expertise and knowledge about a threat. On the other hand, 0-day attacks and recently discovered ones can pass through an IDS undetected, unless their fingerprint is very similar to another one in the intrusion detection system internal database.

To overcome such limitations, current scientific literature started using supervised and unsupervised machine-learning approaches to provide trainable attack detection tools with high accuracy. However, the current state-of-the-art is mostly focused on detecting anomalous traffic [40], without classifying the attacks, and the few articles devoted to attack classification are mostly limited to denial-of-services and volumetric attacks [41] as well as hazard detection and differentiation [42].

2.6. Threat Intelligence and Information Sharing

Security Information and Event Management (SIEM) solutions aim at providing real-time analysis and management of security alerts. They are commonly used in production environments to have a global picture of the security status of an IT infrastructure and can allow administrators to perceive a threat before it can maximize its damage [43].

Despite Internet-of-Things devices are starting to become ubiquitous, however, traditional SIEM systems have limited capacities to interface with IoT devices and embedded systems.

The SIEM will receive relevant structured data from multiple data sources, improving his import capabilities, reducing the number of possible false positives. This will be possible thanks to the adoption of Malware Information Sharing Platform (MISP), extended with the addition of the Trust and Reputation module, which will perform the needed analysis and enrichment before injecting the data into the SIEM itself. Another improvement will be related to the possibility of extracting new IDS rules from these enriched events through MISP, and send them dynamically to the SIEM, exploiting the built-in sharing capabilities of the former.

2.7. Identity Management and Accountability

Current identity Management (IdM) systems are mostly based on centralized solutions, such as corporate directory services, domain name registries, Federated services or certificate authorities. However, these approaches are facing several issues, being fragmented and siloed between various service providers, thus limiting the adoption of a holistic view and delivering poor user experience. The upcoming reliance on billions of IoT devices makes it untenable to have all those devices controlled by a centralized identity provider, since a breach of this provider would be disastrous not only for revealing personal data and misallocation of virtual resources but also for attacking the physical infrastructure including the IoT devices.

The emergence of Distributed Ledger Technology (DLT) offers a promising solution, providing the opportunity for fully decentralized identity management [44]. This technology pushes ownership of identity away from centralized services to the edges, i.e. to individuals, so that the identities themselves are in control [45]. In this way, distributed ledgers provide a means for managing a root of trust with neither centralized authority nor a single point of failure. Recently, the DLT-based IdM solutions have been classified into two main categories: self-sovereign digital identities and decentralised trusted identity. The former applications offer self-sovereign identity through block-chain technology where the owner has control over what information they share without external administrative authority [46], while the latter applications offer centralized service that provide identity proofing through existing identifications, like passport and driving license. With respect to the self-sovereign approaches, there are already a few of them providing authentication and authorization capabilities. Bitid [47] is an open protocol which allows simple and secure user login to cloud/web services by authenticating the user based on the public key and block-chain-based network. The authentication proves the identity of the user to a service by signing a challenge. OpenID [48] is an open protocol that allows a user to authenticate to multiple services without need of creating multiple different identities and passwords. It provides one unique identity to the user from some trusted identity provider which can be used to sign into other OpenID-enabled services. NameID [49] is an experimental technology, based on OpenID, which allows a user to register names which can be associated with user data. This data can be verified by everyone in the block-chain network but cannot be forged or censored by unauthorized attackers and no one can retrieve the data without user consent. Finally, uPort [50] is a platform that allows end users to establish a digital identity which can be used as user identity across multiple services without any passwords. It gives full control of sensitive user data to the user by allowing user to own and control their digital assets, securely and selectively disclose their data to counterparts to access digital service. Moreover, it allows the user to digitally sign and encrypt documents, data, messages, transactions and to send these over the distributed ledger network to interact with decentralized applications.

2.8. Intent-based Services

The automatic network management can reduce network administrator's tasks (network configuration, configuration change, etc.). The automatic network management considers network administrator's intent or policy.

Policy Based Network Management (PBNM [51]) is a technique that enables update of network configurations with network administrator's policies. PBNM enables to define policies, which manage network resources and ensure that network resource is appropriately allocated to users. Policies are formulated using the Event-Condition-Action (ECA) rule and are described using the "if condition then action" rule. The Common Open Policy Service (COPS [52]) protocol has been standardized in the Internet Engineering Task Force (IETF). It has a simple query and response form and exchanges policy information between a policy server and its clients. Recently, Simplified Use of Policy Abstraction (SUPA) working group has discussed data models of policies in the IETF. In conventional management of network states, Simple Network Management Protocol (SNMP) has been widely deployed based on a request-response form. Recently, Network Configuration Protocol (NETCONF [53]) has been discussed in the IETF NETCONF working group. The NETCONF is a management protocol for correcting states of network devices and updating their configuration and is based on an XML form. Yet Another Next Generation (YANG [54]) is a data modelling language used to design configuration and state data on the NETCONF protocol.

The concept of Intent-Based Networking (IBN) has been proposed as a new network management framework in OpenDaylight Network Intent Composition [55]. Intent-based interface has been pursued rigorously by IETF and major open-source project communities (ONF [56], ONOS [57] and OpenDaylight [58]) to provide a standardized intent-based northbound interface for SDN. Intent of a network administrator is used to be expressed in concrete description of configurations stored on devices to update configurations. To describe the intent, the concept of Intent-Based Network Modelling language has been discussed in IETF IB-Nemo [59] BoF, and a draft specification and implementation of it is developed in the NEMO project [60], [61], [62]. Another specification method was also developed by policy graph (e.g., PGA [63]).

2.9. Artificial Intelligence

Network management and orchestration can require real time (latency ~ milliseconds) complex decision making as softwarisation and virtualisation of network resources. The artificial intelligence (AI) techniques enable to analyse historical, temporal and frequency network data. The artificial intelligence techniques, especially machine learning (ML) and statistical learning algorithms [64], can help achieve the FISHY framework to be intelligent as well as autonomous, i.e., to make network self-aware, self-configurable, self-optimization, self-healing and self-protecting systems [65]. The AI-enabled functionalities taking advantage of Intent-based networking, NFV, SDN, network slicing, and security will enable cognitive network management for 5G and

doi:10.20944/preprints202104.0580.v1

beyond. The current development of network management solutions, including CogNet, Selfnet, SONATA and 5GeX [66], are although focused on cognitive network management for 5G devices, the beyond 5G management solutions would require optimizing network as an entity in a secure, resilient and cognitive IoT-fog-cloud infrastructure taking advantage of in-network computing and communication to minimizing the overall energy footprint. However, the success of an intelligent and autonomous system is defined by the AI techniques that can effectively be adopted in different parts of the network management infrastructure. Thus, the intent orchestrator needs to provide not only the handcrafted policies, but also utilizes the power of Big Data, computing dynamic resources, making intelligent decision based on the processed data near the end users, providing low latency as well security as required by critical surveillance, medical and many commercial applications [67]. Moreover, the project will exploit Natural Language Processing (NLP), the science of extracting the intention of text and relevant information from text, to support the management of intents by the Intent-based Resilience Orchestrator block. Some popular "NLP as a service" platforms are: (i) LUIS.ai [68] by Microsoft; (ii) Wit.ai [69] by Facebook; (iii) Api.ai [70] by Google; (iv) Watson [71] by IBM.

For the sake of illustration, Table 1 summarizes the review of the art in the research fields related to the proposed cybersecurity solution.

Table 1. Relevant research areas for IoT complex supply chains including current advances and key issues

Research Area	State-of-the-Art	Key Issues
Information Security Assessment	Device security requirements, environment threat levels, assessment process characterization	Quality of security metrics, metrics properties, general model
Policy-based Systems	Traditional manual configuration or some tools for limited automatization	Full protected scenario, high to low level policies translation in non-simple scenarios, configuration orchestration
Trust Monitoring	Remote attestation procedure (TPM)	Considering virtualized environments, traffic attestation (at packet-node level)
Authentication and Authorization	Edge devices security provisioning is an open challenge	Different authentication levels considering constrained edge systems, distributed data sharing, secure nodes discovery, secure virtualization
Threat and Anomaly Detection	IDS is commonly deployed in IT infrastructures	No trained systems rather limited configurable systems, using ML for training
Threat Intelligence and Information Sharing	SIEM solutions	Current SIEM limitations to face IoT systems, using MISP
Identity Management & Accountability	Centralized solutions, recent DLT based IdM solutions	No holistic view, exploit existing solutions to edge systems
Intent-based services	Current automatized management solutions based on policies or intents	Deploy intent-based solutions to orchestrate security actions in a human friendly scenario
Artificial Intelligence	Several network management solutions and NLP platforms exist, benefiting from AI	Adopting AI to facilitate overall system smartness and autonomy, considering intents orchestration and NLP, deciding where decisions should be taken

3. Architecture for Cybersecurity Provisioning

3.1. Concept and Approach

The proposed FISHY architecture aims at delivering a coordinated cyber resilient platform that would provide the appropriate set of tools and methods towards *establishing trusted supply chains of ICT systems through novel evidence-based security assurance methodologies and metrics as well as innovative strategies for risk estimation and vulnerabilities forecasting leveraging state-of-the-art solutions, leading to resilient complex ICT systems, comprising the complete supply chain, particularly focusing on the IoT devices at the edge and the network systems connecting them*.

Addressing Challenges 1 to 5, the proposed architecture is not envisioned as an incremental integrated cybersecurity solution, but rather as an extensible and programmable framework that can flexibly orchestrate the whole set of ICT systems and security controls. The aim is to provide an innovative cyber resilience framework, where complex ICT systems performance in an entire supply chain may be analysed in terms of security, trust and privacy impact on performance. To this end, the proposed architecture seamlessly combines advancements in several domains, including, Software Defined Networking (SDN), Network Function Virtualization (NFV), intent-based networking, AI-based techniques, and Distributed Ledger Technologies (DLT).

The high-level architecture is depicted in Figure 1.2 where the entire supply chain including the stakeholders is also shown. Each stakeholder participates in the supply chain through resources and infrastructure, from data to IT infrastructure, either as provided by the stakeholder itself, or reachable through other stakeholders via core network and clouds. The main concept relies on designing a security, trustworthy and certification layer, transversal to the whole set of stakeholders in the supply chain intended to make the entire ICT supply chain system resilient, but also to correctly measure the complete security compliance and consequently trigger the required actions (mitigation, reconfiguration, etc.), making sure that guarantees for a certain level of cyber resilience are provided. It is worth mentioning that the proposed solution is envisioned to be deployed on the entire set of devices and systems in the supply chain, most notably including the IoT ecosystem. The latter is including heterogeneous IoT devices at various localities and assumes their connections to gateways or hubs, edge and cloud systems as well the network infrastructure to connect them all. Figure 1.2 also introduces the proposed functional architecture, where four principal functional modules are proposed: Intent-based Resilience Orchestrator and Dashboard (IRO), Security and Certification Manager (SCM), Trust Manager (TM) and the Secure infrastructure Abstraction (SIA). The Figure also shows the key blocks within the SCM module, namely the Secure Assurance & Certification Management and the Enforcement and Dynamic Configuration, as well as the Trust & Incident Manager and the Security & Privacy Data Space Infrastructure both into the TM module. Starting from top to bottom, the Intent-based Resilience Orchestrator and Dashboard (IRO) module is designed to work as the user-centric interface to translating and to orchestrating input actions into intents, to be used by other components. The Security Assurance and Certification Management is responsible for the provision of auditable, evidence-based evaluation and certification of the assurance posture of complex ICT systems, based on identified security claims and metrics, setting the roots for the definition of a pan-European process for certification of devices, processes and systems, as required in today’s in the European market. Trust & Incident manager provides the tools for assessing the security of the stakeholder’s device, component or/and system. The Enforcement & Dynamic Configuration block is responsible for making the entire system cyber resilient, even when including potentially insecure components, based on the concepts of dynamic self-configuration. Security and Privacy Data Space Infrastructure is responsible for the collection and storage of data generated from the devices, processes and components of the stakeholders’ ICT systems being part of the supply

doi:10.20944/preprints202104.0580.v1

chain. Finally, Secure Infrastructure Abstraction (SIA) is the infrastructure-centric interface and works as a data interface between different Edge/IoT or Cloud infrastructures and FISHY platform.

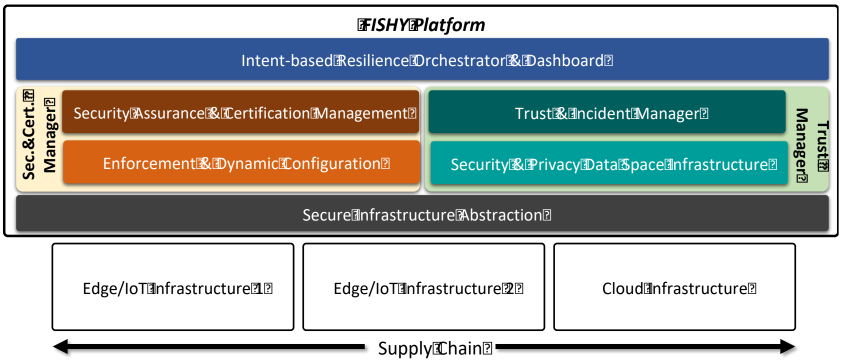
FISHY Platform
Intent-based Resilience Orchestrator & Dashboard
Sec.&Cert. Manager
Security Assurance & Certification Management
Enforcement & Dynamic Configuration
Trust & Incident Manager
Security & Privacy Data Space Infrastructure
Trust Manager
Secure Infrastructure Abstraction
Edge/IoT Infrastructure 1
Edge/IoT Infrastructure 2
Cloud Infrastructure
Supply Chain

Figure Error! No text of specified style in document..**2.** The technical overall concept

A more detailed description of each individual module in the architecture is depicted in Figure 1.3, also including the interaction with the infrastructure along the whole supply chain. Indeed, the whole set of individual components within the modules and blocks defined in Figure 1.2 are represented in Figure 1.3. Each module, block and component are described next to facilitate overall understanding.

3.2. Intent-based Resilience Orchestrator & Dashboard (IRO)

The Intent-based Resilience Orchestrator & Dashboard (IRO) aims at automating the processing, storage and management of intents using Natural Language Processing (NLP) into security workflows, which will be translated to security functions within the FISHY architecture. The processing and optimization of intents use AI while keeping the human-in-the-loop, depending on the desired level of automation, in order to control and enforce a specific workflow being able to react to new threats. The Intent-based Resilience Orchestrator is divided into 6 main components, the Dashboard Interface, Learning & Reasoning, the Knowledge Base, the Intent Manager, Intent Compiler and Monitoring and Telemetry. The main objective of the Dashboard Interface is to provide a unified, harmonized and consistent application, interfacing the human serving as security administrator and the FISHY platform, showing as services, high level policies, risks and vulnerabilities exposure, warnings, performance, metrics, etc. The inputs entered by users of the dashboard will be managed by the rest of components in the IRO. The Learning and Reasoning module uses rule-based AI techniques to learn from the experience acquired in previous executions, considering how the ICT systems react to security alerts, which policies fit better to different scenarios, and learning from feedbacks from other modules. This component generates recommendations for the infrastructure operator to drive automation to dynamically fix policies and optimize the performance of intent manager. The Knowledge base stores the relation between intents, corresponding workflows and security policies. The Intent manager is responsible for handling the intents while checking the conflicting policies and guaranteeing the optimal implementation depending on dynamic rules chosen by the infrastructure operator. The Intent compiler deploys the configuration obtained from the intent manager and will feed other modules in the FISHY architecture. Unlike current commercial solutions, our implementation of Monitoring and Telemetry is: (i) able to dynamically monitor deployment changes enforced by continuous dynamic scheduling, provisioning and auto-scaling, (ii) lightweight yet effective and non-intrusive (iii) independent of a specific infrastructure technology. FISHY will containerise a monitoring and telemetry solution collecting and storing data from different sources, including NFV infrastructure monitoring, Kubernetes infrastructure monitoring, VNF monitoring, SDN monitoring, etc.

3.3. Security Assurance and Certification Manager

Security Assurance & Certification Management is responsible for providing an auditable, evidence-based evaluation and certification strategy for the assurance posture of complex ICT systems, based on identified security claims and metrics, also intended to boot strap the development of new models and tools that would lead to the definition and future establishment of a pan-European process to be followed for the certification of devices, processes and systems in the European market. The set of Security Metrics to be applied on device, component and system level are stored in the respective component, while Security Assurance component is utilized for the proper configuration of the test to be executed against testing procedures and metrics. The real-time, continuous assessment of the security posture of the complex ICT systems will be enabled by a purpose-built Evidence Collection Engine, which will be responsible for aggregating the required evidence from multiple sources related to the operation of individual components, as well as the overarching processes where these components are involved in. This functional group of modules will also include Audit and Certification functions, leveraging the evidence-based approach of the Assurance solution integrated into the platform.

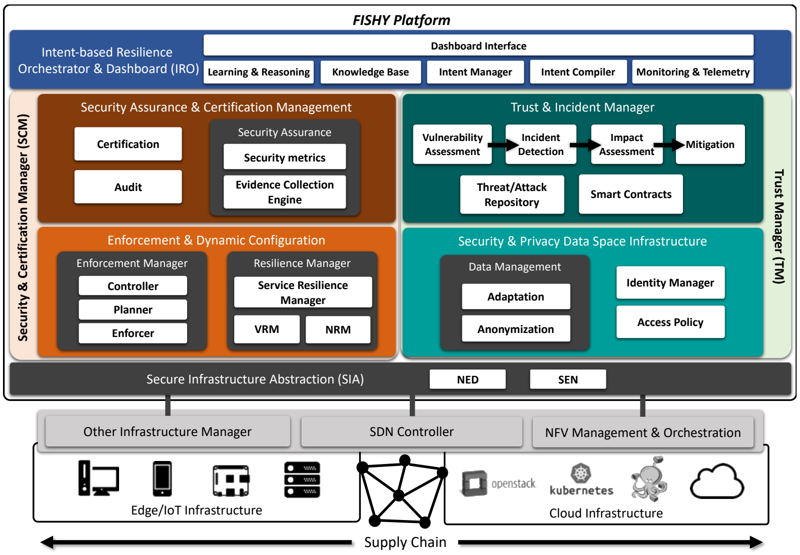

Figure Error! No text of specified style in document.**.3.** FISHY functional

3.4. Enforcement and Dynamic Configuration

The Enforcement and Dynamic Configuration (EDC) block is responsible for making the supply chain measurably reliable end-to-end and assess the reliable and secure operation even in presence of potentially insecure components, based on the concepts of dynamic self-configuration. The general approach includes a predefined set of security features based on an agnostic feature description language. This taxonomy allows to identify and translate dynamically intent-based cybersecurity response into specific configurations. Configurations are applied simultaneously at network topology level and at each Network Security Function (NSF) configuration leveraging the NFV technology. The main components in this functional block are Controller, Planner and Enforcer. Controller is a network controller mapping from the network-specific cyber threat solution to actual NSF deployment and configuration. It can implement changes to the edge network topology and to the configuration of the running NSFs based on the centralized FISHY Intent-based Resilience Orchestration. This element will rely on an existing NFV Orchestrator (NFVO) northbound interface, mapping on it the intent-based security policies to be translated and enforced. Register and Planner is the component where the NSFs will register their security capabilities to be used in enforcement actions, using open standard interfaces, such as I2NSF [14]. The Planner will use this information to combine and decide the best NSFs to use, their topologies, and the configurations to apply. Enforcer is the lower-level block of the EDC, continuously reconfiguring the whole ICT system via the existing NSFs based on the available capabilities. This block will use standard (I2NSF) interfaces to NSFs whenever possible and support specific ones when no standard is available.

3.5. Trust and Incident Manager

Trust & Incident management provides the tools to be used for assessing the security of the stakeholder's device, component or/and system. The Vulnerability Assessment tools will move beyond state-of-the-art (e.g., w3af) providing, among others, automated vulnerability and risks analysis, estimation and detection in source code using Deep Representation Learning techniques. Incident Detection tools will be based on the outcome of vulnerability assessment and will be based on Machine Learning techniques. This component will provide smart processing based on the collected data and it will cover several different research areas. The Mitigation component should be responsible for limiting the scope of the expected impact analysed on the Impact Assessment component. The purpose of all these tools is to provide a cyber-resilience framework that can be quantified, leading to a certification process. The Threat/Attack Repository will store the outcome of the Trust & Incident Management layer whenever the analysis leads to a threat or attack. Based on the immutability principle, the Repository will store the result, so that other stakeholders can be timely informed, and that information can be used for evidence. The Smart Contract is the realization of the component that would alert the stakeholders when a security-related service level agreement is violated.

3.6. Security & Pirivacy Data Space Infrastructure

Security and Privacy Data Space Infrastructure is responsible for the proper collection and storage of data generated from the devices, processes and components of the stakeholders' ICT systems being part of the supply chain. It is based on the concept of distributed, decentralized data storage concept (e.g., IPFS or data lakes) in which users hold a portion of the overall data, creating a resilient system of file storage and sharing. The Data Adaptation component is responsible for the homogenization of data coming at different intervals, in different data models (XML, JSON, small chunks of sensor data, logfiles, etc.) and following different communication means (REST APIs, Pub/Sub, etc.). Moreover, the Identity Manager is based on DLT and is responsible for authenticating the users/processes connected to the Secure and Distributed Data Space, while the Access Policy component caters for preserving privacy per user accessing the data according to specific policies set by the stakeholder responsible for the dataset. In this respect, not all users can access the whole set of data. Finally, the Data Anonymization component takes care of the privacy of the dataset shared by the stakeholders.

3.7. Secure Infrastructure Abstraction (SIA)

The main goal of the Secure Infrastructure Abstraction (SIA) is twofold. On one hand, it is intended to endow IoT systems with as many security guarantees as possible, assuming the inherent trend for IoT or edge devices to be potentially insecure. Two components are considered. The Secure Edge Node (SEN) [72] is a secure software component designed to reside at the edge layer and aimed at providing by default authentication to IoT/edge devices leveraging an extensible blockchain architecture. This architecture provides a totally distributed and fault tolerant chain of trust to IoT/edge devices, to be used to verify device signatures and establish secure TLS connections between the devices. The Network Edge Device (NED) element will be in charge of controlling the network access of the protected environments, providing assurance for traffic flows, and ensuring a proper deployment and topology of the necessary monitoring and threat response functions. FISHY security decisions and actions based on the different framework block insights will be translated into an enforcement configuration in the NED whenever appropriate. On the other hand, the Secure Infrastructure Abstraction provides the proper means to the Enforcement & Dynamic configuration and the Trust & Incident manager to interact with the NFVI resources, regardless of the particular technologies that are used (OpenStack, Kubernetes, AWS, OpenDaylight, ONOS), SDN controllers or other infrastructure managers. A technology agnostic view of the infrastructure is given in FISHY. To this end, API endpoints are exposed that can be used for the management of the network services and VNF instances. The APIs can be further used to collect monitoring data from the NFVIs and the network services, providing useful information about the infrastructure status, allocation of resources for service deployment, VNF performance, etc.

4. Key Business Aspects

4.1. Market Considerations

Cybersecurity is an expanding business in recent years, mainly because IT infrastructure has been the focus part of cyber-attacks, especially when more and more workloads are moving to Cloud and Edge and the risk will continue to growth with IoT adoptions. Moreover, based on OVUM [73] less than 15% of organizations have developed a proactive approach to cybersecurity and digital risk, leaving space for new incomes for solutions such as FISHY.

Additionally, edge computing is ramping up technology in the market with promising revenue streams [74], where operators have a key role, as edge locations owners, as edge connectivity enablers, or as application enablers in edge. None of these potential strategies will succeed without resilience and security included

The unprecedented success of Internet as, not only a global communication tool, but also a powerful and indispensable mean to make business anywhere in the globe has sparked the fast and unstoppable evolution of ICT networks with 5G and IoT as the current main paradigms. Such a hectic pace has brought serious security issues. This, together with the increasing value of the digital assets involved in the daily business processes of companies and the clearer multistakeholder nature of the supply chains, makes ICT networks an appealing target for cyber criminals. Cyber-attacks evolve quickly, and their potential effects are more and more dramatic, to the extent that they could damage entire countries, disrupt national economies and degrade standards of living that were taken for granted. In this eerie scenario, the need for cyber resilient ICT networks pushes the market. New cybersecurity products must address the need to anticipate the threats, absorb the impact of those threats and to respond dynamically to ensure business continuity. The impact of IoT makes the number of devices connected to grow fast, therefore the volume of data flowing skyrockets, and in consequence tracking suspicious data and anomalies becomes very difficult. These challenges the sensing capabilities of the organizations. Besides, privacy and cybersecurity are not a plus anymore, but a responsibility and duty for all the actors of the multistakeholder environment. According to a survey conducted by EY [75] business continuity and disaster recovery resilience have become high priority for the 57% of the respondents, data loss prevention for the 56%, and security awareness and training as means to gain cyber resilience for the 55% There are standards and approaches to cyber resilience promoted by industry, like ISO 23316 which covers the principles and guidelines for organizational resilience. The public sector, and particularly national governments, are getting involved. Such is the case of Scotland, for instance, whose government has created a 3-year programme

(2018-2021) with a set of specific actions to carry out pursuing to grow its national cybersecurity industry [76].

The proposed FISHY architecture is perfectly aligned to this context of strong market demands for products helping increase cyber resilience, which is posed from both the private and public sector, as referred above. FISHY responds to all these needs providing means to achieve higher cyber resilience. On top of this, it enables automatic responses providing the needed intelligence to carry out the self-reconfiguration of the network without the intervention of operators, increasing the promptness and diminishing human errors. Considering the multistakeholder aspect of supply chains, FISHY will address the issues derived from the cascading propagation of the consequences of an attack.

The different stakeholders will benefit from the genuine features of the FISHY components and adopting the framework will open new business opportunities on added-value security services that will become strongly demanded in the market. In short: i) FISHY will bring several competitive advantages to network service providers (NSPs), allowing them to address the requirements of different customers and sectors, to expand their share in the value chain, evolving from network and connectivity providers to cybersecurity service providers; ii) Technology providers and ICT system integrators will benefit from FISHY by means of new and opener ways of collaborating with their network provider customers. thus facilitating their strategic position and gaining an early-entrant advantage within the market of global cybersecurity solutions; iii) Vertical industries will become better enabled to apply advanced security mechanisms to their supply chains, with a better understanding of their features and how they address their requirements, and the possibility of an open, independent verification of security policies, their enforcement and their associated SLAs, and finally; iv) small and medium enterprises will acquire competitive advantages based on their business and market segments and will be provided with a unique opportunity to extend their offerings and business advantages towards an ICT global cybersecurity landscape, supporting new business models to push forward the project's innovations to key security stakeholders.

4.2. Potential Stoppers

Although the benefits brought in by the proposed FISHY architecture in terms of cyber resilience provisioning are quite clear and relevant, some stoppers may hinder a wide adoption of the proposed solution. Particularly, factors that may influence the real FISHY relevance include:

- Low level of awareness about the need for clear responses to cyber threats, often due to a false sense of security, especially at the management level including CEOs and boards of directors, those who have the power to decide on cybersecurity investments.
- Low levels of economic growth, insufficient funding and unexpected interruptions for future and ongoing security innovation initiatives. In the long run, lack of political support for these initiatives could be reflected in insufficient funding but also in failure of efforts devoted to deploying more advanced security management capabilities.
- Misalignments in the technical and business evolution of some of the potential core application environments: energy, industry, health, etc., and including network service provision itself.
- A changing regulatory landscape in network service provisioning and/or security, as response to the development and progress of business models and business opportunities in the new networking market, and technology development itself.

5. Proposed Use Cases

The FISHY architecture is designed aiming at delivering a solution to facilitate the deployment of a cyber resilient platform for supply chains of composed ICT systems. To that end, several real use cases are identified, with two main contributions. First, to assist on the definition of real industry requirements in terms of cybersecurity. Second to facilitate the proper real scenario where the FISHY architecture may be deployed and tested, thus emphasizing the potential benefits of such a deployment. In this section we present three potential use cases, i.e., Farm-to-Fork, Wood-based Panels Trusted Value-Chain and Securing Autonomous Driving Function at the Edge, and we also briefly introduce the expected benefits of the proposed FISHY architecture. Indeed, Table 2 summarizes the expected benefits along with the relevant stakeholders.

Table 2. Use cases benefits and key stakeholders

Use case	Benefits	Stakeholders
Farm-to-Fork	(1) designing a tailored solution for Farm-to-Fork like supply chain scenarios; (2) enabling transactions between actors and devices belonging to different (isolated) IoT silos; (3) enabling trade of resources within the Farm To Fork supply chain in an automated, trusted, and decentralised way; (4) adding an audit service for involved business parties to identify and verify points of failure affecting product quality as products are transported from the farm to the selling point.	Producers, farms, manufacturers, sellers, logistics, and consumers
Wood-based Panels Trusted Value-Chain	(1) enabling security at each integration layer; (2) providing security, integrity and reliability of data flows and systems resilience; (3) ensuring the cybersecurity of all connected devices, preventing attacks and incidents and guaranteeing the availability of the production plants; (4) making the security by design of the different integration layers a must; (5) enabling regular bidirectional data flows with external entities by enforcing the necessary trust levels.	Raw materials suppliers, logistics providers, machinery maintenance companies, industrial clients, cloud provider.
Securing Autonomous Driving Function at the Edge	(1) adding new functionalities (Facial Key and Sensors Secure Environment); (2) certification of the different sensors and actuators integrated in the car; (3) enabling a proper, secure and private data collection; (4) minimizing the security requirements impact on the car by offloading the security applications into the edge.	OEMs, software developers, edge providers, cloud providers, end users, security developers

5.1. Farm-to-fork supply chain (F2F)

During the last years, consumers' demand for "safe" food, including organic, is skyrocketing; thus, producers, manufacturers, sellers and end-users are often struggling to verify the accuracy of data across the whole supply chain of products (from farm to fork). Yet, consumers, especially within such niche markets, like organic food, are increasingly willing to pay for products that provide this information. To date, solutions have revolved around EU certifications and regulations, both of which add costs, are hard to enforce, create everlasting bureaucratic processes, and finally can be confusing to consumers. The challenge here is to obviate the need for a central trusted intermediary and instead develop a decentralised process that, without the need of intermediaries, achieves the same or better (in terms of accuracy, trust, evidence, complexity) functionality as today solutions. In this particular agricultural supply chain scenario, all interested stakeholders will be able to receive information about the conditions under which the products have been cultivated, stored and transported during their entire lifetime. This use case elicits requirements from real supply chain business processes in the agri-food sector that are involved in cultivating, tracking, tracing and selling of perishable goods.

For the sake of overall understanding, the lifecycle of agri-food products, from their production to consumption point runs as follows. Such lifecycle is quite complex and involves a large number of actors and services and may generate a vast amount of data. For example, inside the farm, a perishable product could generate large volumes of related data (e.g., environmental conditions, utilization of fertilizers, date of plantation and harvest, water resources spent). During transportation, data related to the preservation conditions (refrigerator temperature and humidity), shipment details and truck route (GPS data) until final destination can be traced and stored in a distributed ledger, excluding the possibility of non-repudiation. Additionally, data can be created in other intermediary places, such as distribution centers, keeping data with respect to warehouse conditions, final destination, responsible employee, etc. Finally, all the data can be processed, and made available to consumers in the supermarkets

5.2 Wood-based Panels Trusted Value-Chain (WBP TRUST)

Manufacturing of wood-based panels is done in a continuous process involving the feeding of raw materials (wood and resins from external suppliers), their processing (through heat and pressure) and finishing of the panels (sanding and cutting) or further processing (such as surfacing with decorative papers from external suppliers). Panels are then supplied to industrial clients, large or small, in the sectors of furniture manufacturing, flooring production, construction systems or interior design applications (ex: wall panelling).

Requirements from those B2B clients, in terms of product quality, standards compliance and service levels, are more and more demanding. And diversity in the product mix (different sizes, thicknesses, finishes or other product characteristics) is increasing. This context led involved companies to develop manufacturing strategies in novel production plants, aiming at creating a digitally connected and collaborative approach to manufacturing, exchanging data throughout the whole value-chain (upstream and downstream) in a fast, reliable and secure way. This strategy means bridging the gap between two realities – Information Technology (IT) and Operational Technology (OT) – to ensure security, resilience and availability at all levels. This is achieved through an integration architecture that considers different layers, from the shop floor level to a corporate level (holistic view of different production plants), up to the external layer that enables data sharing and automation in a value-chain perspective (from raw materials suppliers, logistics providers and machinery maintenance companies to industrial clients).

Being a rather traditional industry, production plants typically rely on a wide number of different machineries from different suppliers, some of them old and with outdated software, which can pose a challenge when extracting and integrating data from those different parts of the production line and, consequently, sharing that data with value-chain partners. Implementing those novel manufacturing strategies also implies ensuring the connectivity of those machines through sensors and IoT devices to enable data flows at the plant level (manufacturing floor), at the company level (between different plants) and in an ecosystem perspective (with suppliers and clients). This poses great challenges to ensuring the security, integrity and reliability of these data flows and the resilience of the systems in place. Assessing risks and vulnerabilities of all equipment (machinery, sensors, PLCs and others) and ensuring the cybersecurity of all connected devices and, consequently, preventing attacks and incidents and guaranteeing the availability (uptime) of the production plants is of paramount importance. Additionally, and from a value-chain perspective, ensuring the security by design of the different integration layers (at the plant level, at a corporate level and at an external level) is key to foster trust, and stimulate data sharing/mining and value-added services. But the lack of a reference architecture and of a comprehensive framework for value-chain connectivity poses some great challenges to the implementation of such a vision. Currently, data at an OT level is not shared with external entities.

5.3 Securing Autonomous Driving Function at the Edge (SADE)

With the increasing number of electronic, intelligent embedded systems and connectivity in the Cars plus the impending revolution of the fully connected and autonomous cars, Security is becoming a major concern in the industry, regulators and the public [76]: "*84-percent of automotive professionals have concerns that their organizational cybersecurity practices are not keeping pace with evolving technologies reveals securing the Modern Vehicle: A Study of Automotive Industry Cybersecurity Practices, a report released by Synopsys and SAE Internationa*l".

In practice, aspects widely adopted by manufacturers showing strong concerns about cybersecurity fall around Software in the Automotive Supply Chain and level of the connectivity in the Connected Car. On one hand, OEMs rely on hundreds of providers for many of the embedded systems. This requires controlling hundreds of different software versions within the car, posing challenges around SW verifications and attestation and how to regularly maintain and patch this software and integrate them in and unified way within the automobile cybersecurity framework. On the other hand, automobile systems are now more exposed to the remote risks and tampering.

In order to tackle these two major challenges, OEMs are introducing more complex systems into the cars, such as Firewalls and Gateways, new systems that are also prone to risks, updates and maintenance by the OEMs. Besides best practices, such as security testing prior to release, patching or managing a homogenous/consistent secure software development life cycle become more and more challenging. Usually, industry relies on patching, dynamic security testing and penetration testing during its development phase to address some of them, but once the car is released the increasing volume of electronic (sensors, actuators, gateways, firewalls and ECUs) makes difficult to maintain (i.e., development and patching) the systems. This also leads to concerns about new functions that OEMs may consider deploying, especially when sensitive user information is stored in any embedded system, this apply specially to any biometric information of the user. In this context, the Automobile industry tens to shift most of the intelligence to the cloud in order to simplify the car electronic. This trend is being boosted by upcoming technologies such as 5G, C-V2X, 802.11P and Edge computing.

6. Conclusions

This paper puts the focus on a highly attractive scenario, that is cyber resilience provisioning in supply chains built on complex ICT systems. The contribution starts by identifying key challenges still demanding specific attention by the scientific community, justified by a thorough review of the current literature in those key research areas strongly linked to the main objective. Then, on a technical view, the paper introduces a functional architecture aimed at addressing the specific challenges previously identified by that particular supply chain context.

Beyond the functional architecture definition, it is worth mentioning the use case scenarios shown as key examples where the proposed architecture may be deployed at, as well as the benefits such a deployment may bring in to these scenarios, what indeed, is the main rationale for the architecture definition.

This paper may be read as both a wide survey of existing contributions in the well identified research areas aligned to the main supply chain paper target as well as, a benchmarking report in terms of either architectural design and/or real benefits for other similar initiatives.

Author Contributions: Conceptualization, X.M., E.M., J.R., A.J., P.T., A.C., A.L., D.L., and H.S..; methodology, X.M., E.M., P.T., and J.R.; investigation, X.M., E.M., A.J., and P.T; writing—original draft preparation, X.M. and E.M.; writing—review and editing, X.M., E.M., J.R., A.J., P.T., A.C., A.L., D.L., H.S., A.G., A.S., J.S., and G.K.; project administration, X.M., and J.R.; funding acquisition, X.M. and E.M. All authors have read and agreed to the published version of the manuscript

Funding: This research was funded by H2020 FISHY Project, grant number 952644, and for UPC authors by the Spanish Ministry of Science, Innovation and Universities and FEDER, grant number RTI2018-094532-B-I00

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

Abbreviations

The next abbreviations are used in this paper.

AI	Artificial Intelligence
AWS	Amazon Web Services
B2B	Business to business
COPS	Common Open Policy Service
DLT	Distributed Ledger Technology
ECA	Event-Condition-Action
EDC	Enforcement and Dynamic Configuration
F2F	Farm-to-Fork
IBN	Intent-Based Networking
ICT	Information and Communication Technologies
IdM	Current identity Management
IDS	Intrusion Detection Systems
IETF	Internet Engineering Task Force
IoT	Internet of Things
IPFS	InterPlanetary File System
IPS	Intrusion Prevention Systems
IPSec	Internet protocol Security
IRO	Intent-based Resilience Orchestrator and Dashboard
IT	Information technology
JSON	JavaScript Object Notation
MAC	Media Access Control
MDGSM	Method for Designing Good Security Metrics
MISP	Malware Information Sharing Platform
ML	Machine Learning
NED	Network Edge Device
NETCONF	Network Configuration Protocol
NFVO	NFV Orchestrator
NFV	Network Function Virtualization
NIST	US National Institute for Standards and Technology
NLP	Natural Language Processing
NSF	Network Security Function
NSP	Network Service Provider
OEM	Original Equipment Manufacturer
ONOS	Open network Operating System
OT	Operation technology
PBNM	Policy Based Network Management
PLC	Programmable Logic Controller
SADE	Securing Autonomous Driving Function at the Edge
SCM	Security and Certification Manager
SDN	Software Defined Networking
SEN	Secure Edge Node
SIA	Secure infrastructure Abstraction
SIEM	Security Information and Event Management
SNMP	Simple Network Management Protocol
SME	Small and Medium Enterprise

SUPA	Simplified Use of Policy Abstraction
TLS	Transport layer Security
TM	Trust Manager
TPM	Trusted Platform Module
VNF	Virtualized Network Function
WBP TRUST	Wood-based Panels Trusted Value-Chain
XML	Extensible Markup Language
YANG	Yet Another Next Generation

References

1. https://www.thesslstore.com/blog/the-rise-of-cyber-resilience/, available online [accessed April 16, 2021]
2. R. Ross, R. Graubart, D. Bodeau and R. McQuaid, *Systems security engineering: Cyberresiliency considerations for the engineering of trustworthy secure systems*, vol. 2, National Institute of Standards and Technology, 2018
3. "WannaCry ransomware attack,", https://en.wikipedia.org/wiki/WannaCry_ransomware_attack, available online [accessed April 16, 2021]
4. Accenture,"Exploring Consumers' Digital Trust, https://www.accenture.com/us-en/insight-accenture-health-2017-consumer-survey, available online [accessed April 16, 2021]
5. Kevin Orrey "Cyber Attack: Exploiting the User - There are so many ways!", MSc Computer Security and Forensics Masters Thesis Report, University of Bedfordshire, 2010
6. From the Puget Sound Business Journal: http://www.bizjournals.com/seattle/print-edition/2013/02/15/lithium-ion-battery-technology-has.html, Feb 15, 2013, 3:00am PST, Boeing 787 battery lags behind evolving lithium-ion technology
7. Urciuoli, Männistö, Hintsa & Khan, vol.29, http://dx.doi.org/10.11610/isij.2904 2013, 51-68 SUPPLY CHAIN CYBER SECURITY – POTENTIAL THREATS
8. Development of a Strategic Roadmap Towards a Large Scale Demonstration Project in European Logistics and Supply Chain Security, LOGSEC Deliverable, 31 March 2011, www.logsec.org/images/upload/file/docs_logsec-roadmap-finalpublic.pdf
9. https://www.appknox.com/resources#0, available online [accessed April 16, 2021]
10. Gemalto, "Breach Level Index 2017 - H1 Report", 2017.
11. K.W. Hamlen, "Stealthy Software: Next-generation Cyber-attacks and Defenses", International Conference on Intelligence and Security Informatics, DOI:10.1109/ISI.2013.6578797.
12. Independent IT Security Institute, AVTest, Statistics report, https://www.av-test.org/en/statistics/malware/, available online [accessed April 16, 2021]
13. X. Masip-Bruin, Guang-Jie Ren, R. Serral-Gracia, and M. Yannuzzi, "Unlocking the Value of Open Data with a Process-based Information Platform," presented in IEEE CBI 2013, Vienna, Austria, July 2013
14. D. Monahan, EMA Report Summary: Achieving High-Fidelity Security, 2016, accessed at https://www.savvius.com/wp-content/uploads/2017/07/EMA_Savvius_High_Fidelity_Security_2016.pdf
15. Research Reveals Organizations Falling Behind in Cybersecurity Analytics and Operations Despite Business Pressure to Improve, Businesswire, 2017
16. https://www.gartner.com/en/newsroom, available online [accessed April 16, 2021]
17. S.Kahvazadeh, V.Barbosa, X.Masip-Bruin, E.Marín-Tordera, J.Garcia, R.Diaz, "Securing combined Fog-to-Cloud System through SDN approach", 4th Workshop on CrossCloud Infrastructures & Platforms (ACM Digital Library), Serbia, Belgrade, April 2017
18. Protection, R. L.-I. J. of C. I., & 2018, undefined. (n.d.). Standards on cybersecurity assessment of smart grid. *Elsevier*. Retrieved from https://www.sciencedirect.com/science/article/pii/S1874548216301421
19. Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (n.d.). *Special Publication 800-115 Technical Guide to Information Security Testing and Assessment Recommendations of the National Institute of Standards and Technology*.
20. Pendleton, M., et al (2016). A Survey on Systems Security Metrics. *ACM Computing Surveys*, *49*(4), 1–35.
21. Yee, G. O. M. (2019). Designing Good Security Metrics. In *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)* (pp. 580–585). IEEE. https://doi.org/10.1109/COMPSAC.2019.10270
22. Wang, L., Jajodia, S., & Singhal, A. (2017). *Network Security Metrics*. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-66505-4
23. Yee, G. O. M. (2019). Designing Good Security Metrics. In *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)* (pp. 580–585). IEEE. https://doi.org/10.1109/COMPSAC.2019.10270
24. Behi, M., et al., (2018). A New Approach to Quantify Network Security by Ranking of Security Metrics and Considering Their Relationships. *International Journal of Network Security*, *20*(1), 141–148. https://doi.org/10.6633/IJNS.201801.20(1).15
25. Aldya, A. P., et al, (2019). Measuring effectiveness of control of information security management system based on SNI ISO/IEC 27004: 2013 standard. *IOP Conference Series: Materials Science and Engineering*, *550*, 012020.
26. Houngbo, P. J., & Hounsou, J. T. (2015). Measuring information security: understanding and selecting appropriate metrics. *International Journal of Computer Science and Security (IJCSS)*, *9*(2), 108.
27. Bhol, S. G., et al., (2020). Cybersecurity Metrics Evaluation Using Multi-criteria Decision-Making Approach. In *Smart Intelligent Computing and Applications. Smart Innovation, Systems and Technologies* (pp. 665–675).

28. R. Craven, J. Lobo, E. Lupu, A. Russo, M. Sloman, “Security policy refinement using data integration: a position paper”, Second ACM workshop on assurable and usable security configuration, DOI: 10.1145/1655062.1655068
29. R. Laborde, M. Kamel, F. Barrère, A. Benzekri, “Implementation of a Formal Security Policy Refinement Process in WBEM Architecture”, Journal of network and systems management, DOI: 10.1007/s10922-007-9063-z
30. W. Han, C. Lei, “A Survey on Policy Languages in Network and Security Management”, Computer Networks, DOI: 10.1016/j.comnet.2011.09.014
31. https://www.snort.org/, available online [accessed April 16, 2021]
32. https://suricata-ids.org/, available online [accessed April 16, 2021]
33. http://www.trustedcomputinggroup.org/, available online [accessed April 16, 2021]
34. E. Cesena, G. Ramunno, R. Sassu, D. Vernizzi, A. Lioy, “On scalability of remote attestation”, Sixth ACM workshop on scalable trusted computing, DOI: 10.1145/2046582.2046588
35. R. Sailer, X. Zhang, T. Jaeger, L. Van Doorn, “Design and implementation of a TCG-based integrity measurement architecture”, Conference on USENIX security symposium
36. https://tools.ietf.org/html/rfc5246, and https://tools.ietf.org/html/draft-ietf-tls-tls13-28, available online [accessed April 16, 2021]
37. https://tools.ietf.org/html/rfc6071, available online [accessed April 16, 2021]
38. Adat, V., & Gupta, B. B. (2018). Security in Internet of Things: issues, challenges, taxonomy, and architecture. Telecommunication Systems, 67(3), 423–441.
39. https://www.bro.org/, available online [accessed April 16, 2021]
40. T. Shon, J. Moon, “A hybrid machine learning approach to network anomaly detection”, Information sciences, DOI: 10.1016/j.ins.2007.03.025
41. C. Livadas, R. Walsh, D. Lapsley, W. T. Strayer, “Using Machine Learning Techniques to Identify Botnet Traffic”, Conference on Local Computer Networks, DOI: 10.1109/LCN.2006.322210
42. A.Moradbeikie, K.Jamshidi, A.Bohlooli, J.Garcia, X.Masip, "An IIoT based ICS to improve safety through fast and accurate hazard detection and differentiation", IEEE Access, Vol. 8, 2020, pp. 206942-206957, doi: 10.1109/ACCESS.2020.3037093
43. Konstantina Fotiadou, et al, “Incidents Information Sharing Platform for Distributed Attack Detection”, IEEE Open Journal of the Communications Society, vol. 1, pp. 593-605, 2020
44. D. Lagutin et al, “Secure open federation of IoT platforms through interledger technologies-the SOFIE approach”, Proceedings of the European Conference on Networks and Communications (EuCNC), pp. 518-522, 2019
45. L-D Ibáñez, et al., “Redecentralizing the Web with Distributed Ledgers”, IEEE Intelligent Systems, Vol.: 32-1, Jan.-Feb. 2017
46. P. Dunphy, F. Petitcolas, “A First Look at Identity Management Schemes on the Blockchain”, IEEE Security and Privacy Magazine, special issue on "Blockchain Security and Privacy”, 2018
47. E. Larchevêque, “Bitcoin address authentication protocol (bitid)”, August 2016, https://github.com/bitid/bitid/blob/master/BIP_draft
48. What is openid? | openid, 2005. http://openid.net/get-an-openid/what-is-openid/, available online [accessed April 16, 2021]
49. D. Kraft, “Nameid: Your crypto-openid”, 2013. https://nameid.org/
50. C. Lundkvist, R. Heck, J. Torestensson, Z. Mitton, M. Sena, “Uport: A platform for self-sovereign identity. Technical report, October 2016, http://whitepaper.uport.me/uPort_whitepaper_DRAFT20161020.pdf.
51. B. Raouf, I. Aib, “Policy-based management: A historical perspective,” JNSM 15.4, pp.447-480, 2007
52. J. Walker, A. Kulkarni, “Common Open Policy Service (COPS) Over Transport Layer Security (TLS),” RFC4261, 2005
53. R. Enns, M. Bjorklund, et al, “NETCONF Configuration Protocol,” RFC6241, 2011
54. M. Bjorklund, “YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF),” RFC6020, 2010
55. OpenDaylight, “Network Intent Composition:Main,” https://wiki.opendaylight.org/view/Network_Intent_Composition:Main
56. Open Networking Foundation., “Project boulder: Intent northbound interface (nbi).”, https://github.com/OpenNetworkingFoundation/BOULDER-Intent-NBI, available online [accessed January 8, 2021]
57. P. Berde et al., “ONOS: Towards an open, distributed sdn os,” in Proceedings of the Third Workshop on Hot Topics in Software Defined Networking, ser. HotSDN ’14. New York, NY, USA: ACM, 2014, pp. 1–6.
58. The OpenDaylight Project, Inc., https://www.opendaylight.org, available online [accessed April 16, 2021]
59. Ibnemo, “About Ibnemo,” https://www.ietf.org/mailman/listinfo/ibnemo, available online [accessed April 16, 2021]
60. OpenDaylight, “NEMO:Main,” https://wiki.opendaylight.org/view/NEMO:Main]
61. S. Hares, “Intent-Based Nemo Overview,” IETF Internet-Draft draft-hares-ibnemo-overview-01, Apr. 2016, work in Progress
62. Y. Zhang et al., “NEMO (NEtwork MOdeling) Language,” Internet Engineering Task Force, Internet-Draft draft-xia-sdnrg-nemo-language-04, Apr. 2016
63. C. Prakash et al., “Pga: Using graphs to express and automatically reconcile network policies,” in Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication, ser. SIGCOMM ’15. New York, NY, USA: ACM, 2015, pp. 29–42.
64. P. Trakadas, et al, “An Artificial Intelligence-Based Collaboration Approach in Industrial IoT Manufacturing: Key Concepts, Architectural Extensions and Potential Applications” Sensors, vol. 20, issue 19, pp. 5480, 2020
65. J.O. Kephart and D.M. Chess. “The Vision of Autonomic Computing” IEEE, 2013 http://ieeexplore.ieee.org/document/1160055/
66. A white paper by 5GPPP Network Management & Quality of Service Working Group, “Cognitive Network Management for 5G,” Available online: https://5g-ppp.eu/wp-content/uploads/2017/03/NetworkManagement_WhitePaper_1.pdf

doi:10.20944/preprints202104.0580.v1

67. O. Abdelkhalek et al, ‘‘A genetic algorithm for a multi-objective nodes placement problem in heterogeneous network infrastructure for surveillance applications,’’ in Proc. IFIP WMNC, Oct. 2011, pp. 1–9
68. Microsoft Language Understanding (LUIS), https://www.luis.ai/home, available online [accessed April 16, 2021]
69. Facebook Wit.ai, https://wit.ai/, available online [accessed April 16, 2021]
70. Google Api.ai, https://dialogflow.com, available online [accessed April 16, 2021]
71. IBM Watson, https://www.ibm.com/watson, available online [accessed April 16, 2021]
72. M.Miquel, E.Marín-Tordera, X.Masip-Bruin, S.Sánchez-López, J-García, "Implementing a Blockchain-based Security System Applied to IoT", Broadnets, LNICST 335, pp.1-11 (2021), December 2020
73. OVUM, 2019 Trends to Watch: Cybersecurity, https://ovum.informa.com/resources/product-content/2019-trends-to-watch-cybersecurity-int003-000295, available online [accessed April 16, 2021]
74. Analysys mason, 20 November 2018, Opportunities and threats for operators in the edge computing value chain, https://www.analysysmason.com/Research/Content/Reports/edge-computing-report-RMA16/, available online [accessed April 16, 2021]
75. EY Global Information Security Survey (GISS). Report 2016
76. Scottish Government: “Cyber resilience economic opportunity: key actions 2018-2021). ISBN 9781787811775, https://www.sae.org/binaries/content/assets/cm/content/topics/cybersecurity/securing_the_modern_vehicle.pdf, available online [accessed April 16, 2021]