applied sciences

MDPI

Article

Future Industrial Networks in Process Automation: Goals, Challenges, and Future Directions

Johan Åkerberg [1,*], Johan Furunäs Åkesson [2], Jorgen Gade [3], Maryam Vahabi [1,3], Mats Björkman [1], Mehrzad Lavassani [1,4], Rahul Nandkumar Gore [1], Thomas Lindh [5] and Xiaolin Jiang [3]

[1] Division of Networked and Embedded Systems, Mälardalen University, 721 23 Västerås, Sweden; maryam.vahabi@mdh.se (M.V.); mats.bjorkman@mdh.se (M.B.); mehrzad.lavassani@ri.se (M.L.); rahul.nandkumar.gore@mdh.se (R.N.G.)
[2] Westermo Network Technologies AB, 721 30 Västerås, Sweden; johan.furunasakesson@westermo.com
[3] ABB AB Corporate Research, 721 78 Västerås, Sweden; jorgen.gade@se.abb.com (J.G.); xiaolin.jiang@se.abb.com (X.J.)
[4] Division of Industrial Systems, RISE-Research Institutes of Sweden, 852 33 Sundsvall, Sweden
[5] Iggesund Paperboard, 825 80 Iggesund, Sweden; thomas.lindh@holmen.com
* Correspondence: johan.akerberg@mdh.se

Abstract: There are many initiatives and technologies working towards implementing factories of the future. One consensus is that the classical hierarchical automation system design needs to be flattened while supporting the functionality of both Operation Technology (OT) and Information Technology (IT) within the same network infrastructure. To achieve the goal of IT/OT convergence in process automation, an evolutionary transition is preferred. Challenges are foreseen during the transition, mainly caused by the traditional automation architecture, and the main challenge is to identify the gap between the current and future network architectures. To address the challenges, in this paper, we describe one desired future scenario for process automation and carry out traffic measurements from a pulp and paper mill. The measured traffic is further analyzed, which reveals representative traffic characteristics in the process automation. Finally, the key challenges and future directions towards a system architecture for factories of the future are presented.

Keywords: industrial network; process automation; IT/OT convergence; time-sensitive networking

Citation: Åkerberg, J.; Furunäs Åkesson, J.; Gade, J.; Vahabi, M.; Björkman, M.; Lavassani, M.; Nandkumar Gore, R.; Lindh, T.; Jiang, X. Future Industrial Networks in Process Automation: Goals, Challenges, and Future Directions. *Appl. Sci.* **2021**, *11*, 3345. https://doi.org/10.3390/app11083345

Academic Editors: Paula Fraga-Lamas, Tiago M. Fernández-Caramés and Sérgio Ivan Fernandes Lopes

Received: 12 March 2021
Accepted: 6 April 2021
Published: 8 April 2021

1. Introduction

Future digitalization of the process industry by connecting more advanced and powerful technologies like cloud computing and machine learning is expected to increase production efficiency. As a response to the envisioned effects of the integration of new technologies in the automation systems, several initiatives such as Industry 4.0, Industrial Cyber-Physical Systems (CPSs), and Industrial IoT systems have been formed to respond to the needs, to mention a few [1–4]. Furthermore, research towards closing the large gap with respect to interoperability is also ongoing, such as OPC Unified Architecture (OPC UA) [5,6]. In order to harvest the envisioned effects, it has to be assumed that any information can easily be accessed from everywhere, independent of residing in Information Technology (IT) or Operational Technology (OT) systems. Therefore, it is paramount to reduce or even eliminate the boundaries between IT and OT subsystems to pave the way for innovations, new products, and services towards higher automation levels.

However, with the existing traditional architecture, the automation pyramid, the possibilities are limited. The automation pyramid, illustrated in Figure 1, shows a typical example of today's architecture in existing industrial automation installations. This architecture has been widely adopted, evolved, and implemented in the last 30 years, accompanied by hierarchical, diverse, and domain-specific communication structures. This implies that there is a large installed base that cannot easily replace the automation systems and

network infrastructures in one maintenance task with the latest technologies. In order to benefit and increase the probability of adaption in the installed base, e.g., brown-field installations, a stepwise introduction would be beneficial. The COVID-19 pandemic has further pushed the need for stepwise upgrades due to the fact that all personnel cannot be on-site, thus, many need to solve their daily tasks remotely.

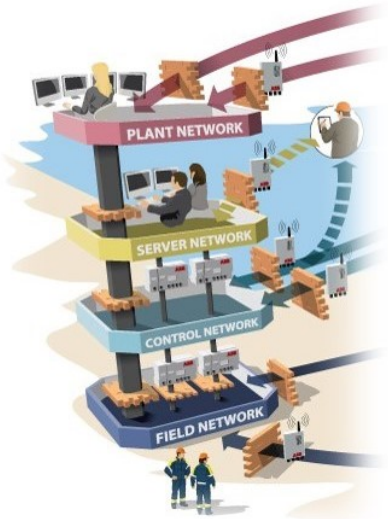

Figure 1. The traditional and hierarchical automation pyramid that has been the de facto standard for three decades.

As the traditional automation pyramid serves its purpose with respect to safety, fault containment, and enforcing traffic types into dedicated levels in order to meet requirements such as availability, deterministic behavior, and high throughput, the integration of new high-level functionality is hard to achieve. New functionality that requires (new) information from the factory floor imposes certain challenges. This is mainly because the networks at the lowest levels have real-time requirements, and in order to guarantee deterministic behavior, other unrestricted traffic is typically not allowed, or not even possible.

The desired network architecture design that accommodates both IT and OT traffic on the same platform is illustrated in Figure 2, where a single bus is shared by different services on time-stringent OT network components (e.g., Field Communication Interface (FCI), dedicated I/O devices, Centralized Network Configuration (CNC), Human Machine Interface (HMI)) and IT network entities (e.g., Enterprise Resource Planning (ERP), Manufacturing Execution Systems (MES)). In fact, customers aim at increasing operational efficiency by decreasing downtime, providing interoperability for the best of the breed, and increasing flexibility and portability. This can be further translated into collapsing multiple one-purpose networks that carry dedicated protocols into one general purpose network that can accommodate both IT and OT traffic in the same infrastructure.

However, this imposes new challenges and ways of working when deploying converged networks. Especially, priorities, Quality of Service (QoS) levels, as well as avoidance of bottleneck links have to be carefully handled, since all traffic classes and traffic types need to coexist while meeting the sum of all requirements to have a sustainable production plant. This task may be difficult even in a green-field scenario, where the latest technology can be installed and commissioned without previous systems that impose constraints. In the brown-field scenario, it is even more challenging, as one may not know what traffic exists and where or how close to the capacity ceiling the network is. Having actual traffic performance from actual installations will guide the research in the green-field scenario and is essential in brown-field scenarios. By ensuring the overall network performance, it would be possible to enable new services and business opportunities by unlocking stranded information and letting, for example, mobile operators and maintenance personnel have access to relevant information from the converged network. This is not an easy task in

itself. However, the Return-on-Investments (RoI) of the installed base has to be considered as well to enable a step-by-step transition towards the future industrial networks.

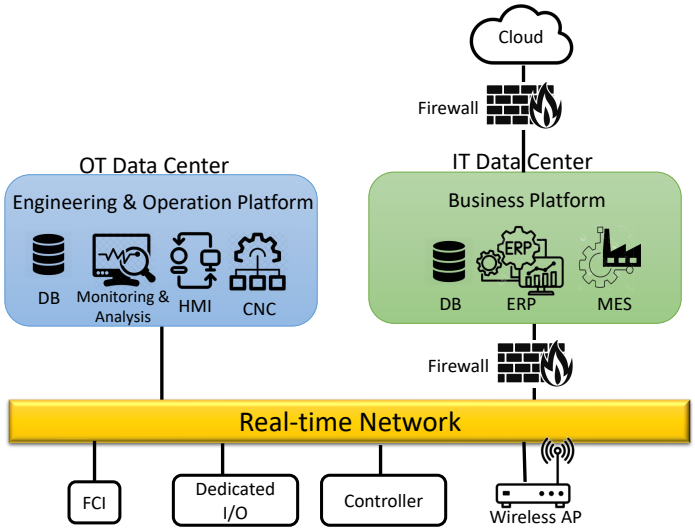

Figure 2. The future control architecture.

In addition, the integration of IT and OT in the traditional and hierarchical architecture is hard to achieve since bypassing of levels is not supported by the system architecture. Besides, identifying the gap between the new architecture and the traditional one is exceptionally challenging. This makes it difficult for the existing architectures to simply adapt to the evolving opportunities in ICT technology [7].

This paper aims to discuss challenges that will be encountered through the evolution process of the industrial networks towards converged networks. By analyzing real traffic from a typical installation in the process industry, we present challenges that have to be addressed and solved. Based on the identified challenges and gaps, we shed some light on future research directions to safeguard the installed base and the RoI in the process industry.

The next section presents the analysis of the current state of a control network and characteristics of the existing traffic flows in a case-study. Section 3 gives an overview of the relevant technologies that aim to realize the IT/OT integration. In Section 4, challenges along the way of the network evolution from guidelines, security, engineering tools, reliability, distributed real-time, and synchronization aspects are discussed. Deriving from the discussed challenges, Section 5 identifies some research directions that can address these challenges, before Section 6 concludes the paper.

2. A Case Study: Iggesund Paperboard

We aim to discuss the challenges in the transformation of existing industrial networks to future converged networks. The knowledge gained from brown-field performance in terms of bandwidth consumption and attributes of various components in the network provides grounds for further integration as well as additional insights for requirement estimation of the green-field installation. For these reasons, we first start with analyzing the current state of an automation network to investigate how characteristics of communication flows contribute to challenges on the transformation path. We perform a case study at Iggesund Paperboard, which is a representative process automation plant. Iggesund Paperboard is a fully integrated pulp and paperboard mill with a long history. There exist two paperboard machines that produce high-quality virgin fiber paperboard for packaging and graphical purposes. One of the paperboard machines can be seen in Figure 3. Multiple control networks coordinate to control the whole production process.

Figure 3. A paperboard machine at the Iggesund paperboard mill.

2.1. Iggesund Production Network

In this study, we focused only on the paperboard machinery production network and limited our investigation exclusively to the server and control network traffic, as illustrated in Figure 1. The production network at Iggesund uses a hot-standby redundancy method, where the secondary (backup) network will be activated if the primary network paths fail. Three marshaling rooms and a number of switches located in different locations across the factory provide the communication backbone for the two paperboard machines. It is worth mentioning that we cover only a small part of the overall OT network that consists of five different control systems from various vendors and generations, 43 operator and engineering stations connected to the server network, and 32 process controllers and PLC on various Virtual Local Area Networks (VLANs).

The network topology is illustrated in Figure 4, which is composed of multiple control network VLANs and one server network VLAN (client/server VLAN). The server network VLAN is connected to the IT network via a firewall. For the sake of privacy, we replace the real VLAN identifier values with letters and present them in letters throughout this section.

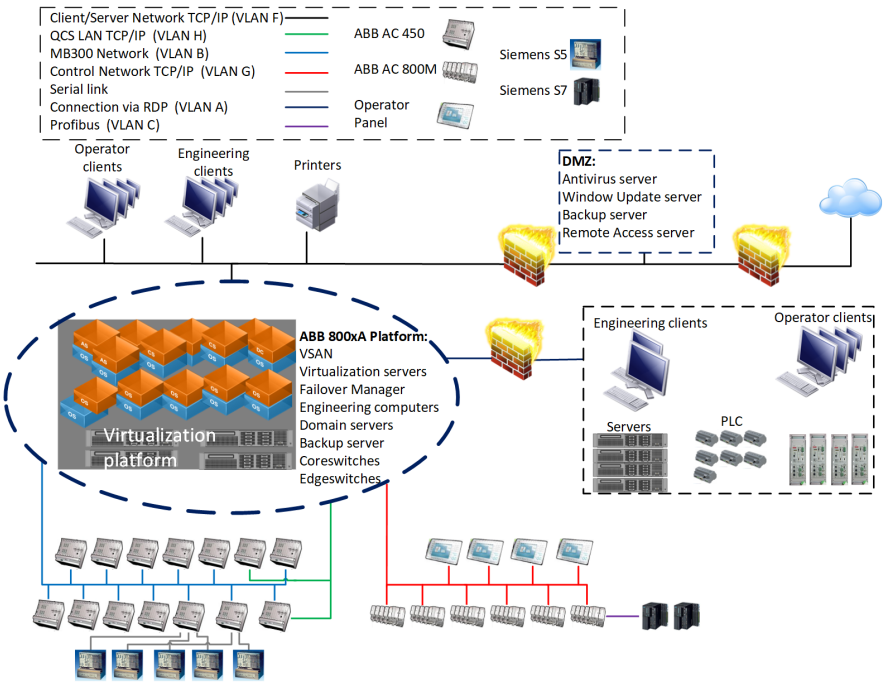

Figure 4. Network topology of one of the paperboard machines at Iggesund.

2.2. Traffic Analysis

To have a complete view of the OT network traffic flows, we captured the traffic during paperboard production using a traffic recorder connected to both the primary and the backup network at the same time. On each of the connected ports from the recorder, traffic mirroring was enabled, such that all traffic in that switch was mirrored to the traffic recorder. The limitation of this capturing method is that it is not sure that all traffic flows in the ring network were captured. However, due to the large distances and different rooms, it was not possible to mirror the traffic from all switches in both the primary and backup network concurrently. Although not a perfect method, it was the only viable solution and provided as much insight as possible into an OT core network during production. The data set contains both the primary and secondary network during 12 h with a size of 60 GB.

One of the fundamental analyses is the number of traffic flows and what nodes are contributing to the network. Figure 5 aims to visualize the communication flows as colored lines per VLAN and colored dots as nodes in the corresponding VLANs. The network comprises 337 unique communication flows, representing the communication between nodes and control systems. Unique communication flows for each node vary from 1 to 108, which is a maximum of 107 communication destinations for the control system. In this figure, we can clearly see that there are two communication flows clusters. The two larger structures in the figure show that the controllers communicate with the connectivity server, which is illustrated as a virtualization platform in Figure 4. The other large portion of flows represents the case when operator stations and engineering stations are communicating with the connectivity server. The connectivity server is a gateway between the control network and the server network. The connectivity server provides protocol translation from various controller protocols used and provides an open platform communication interface for the server network. The connectivity server also creates a boundary between real-time traffic and relaxing timing requirements to the server network.

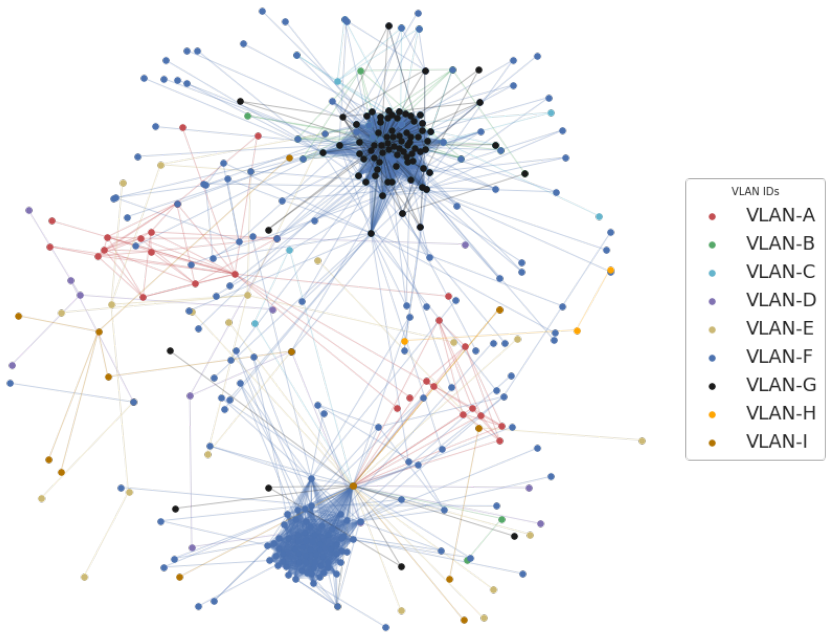

Figure 5. Traffic flows from one of the paperboard machines during recording hours.

A pragmatic approach towards the evolution of the process industry is to characterize various traffic flows and identify appropriate traffic classifications to map the flows into the correct traffic type. Figure 6 shows the traffic load over one second per VLAN. It can be seen that there are a few VLANs with a consistent amount of traffic over time, and some vary a lot over time. The VLANs with a steady amount of traffic are most likely handling periodic transmissions to and from the controllers, e.g., control network traffic. VLANs

with a fluctuating network load are more difficult to classify in this way, as they might contain both periodic and aperiodic traffic. Those VLANs require a more in-depth analysis in order to be classified correctly. As previously mentioned, the control networks should have predictable network utilization over time. Figure 7 illustrates this expected behavior with a limited range in both packet size and the number of packets per second, as well as the contribution of different protocols in the VLAN.

In Figure 8, the number of packets and the amount of data transmitted in the server network (VLAN-F) is shown as well as the distribution of different protocols. In this VLAN, it can be observed that both the number of transmitted packets and the average size of the payload vary over time. However, from the lower part of the figure, it can be seen that approximately 2000 packets per second is a base-load, with occasional traffic peaks. This behavior could be explained by the fact that the operator stations are subscribing for periodic status updates with a limited variation in packet size, from connectivity servers. The periodic updates would then serve as the base-load in the server network. The variations are then an aggregate of the various protocol types shown on the right-hand side. An example of sporadic traffic is when the operators change the process views on their screens to a different section of the process. This change causes traffic bursts due to requests to start and stop subscriptions of information corresponding to the previous and new process view. Another example can be when the operators transmit and receive production data to the Manufacturing Execution System (MES) or other information to file servers or similar. Generally, this sporadic traffic has a larger packet payload, shown in Figure 8.

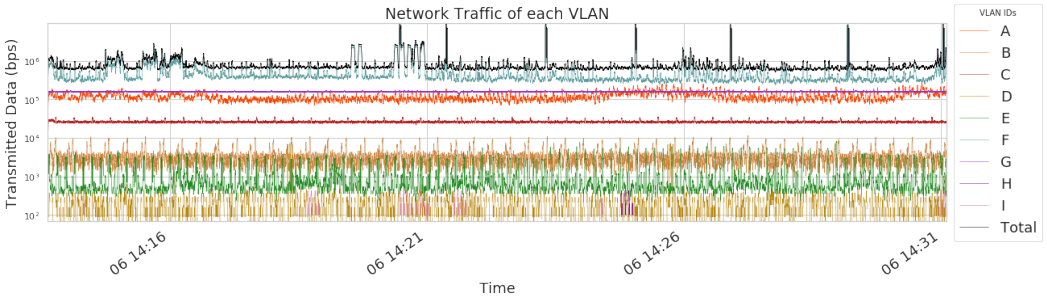

Figure 6. Traffic per Virtual Local Area Network (VLAN); illustrated in logarithmic scale.

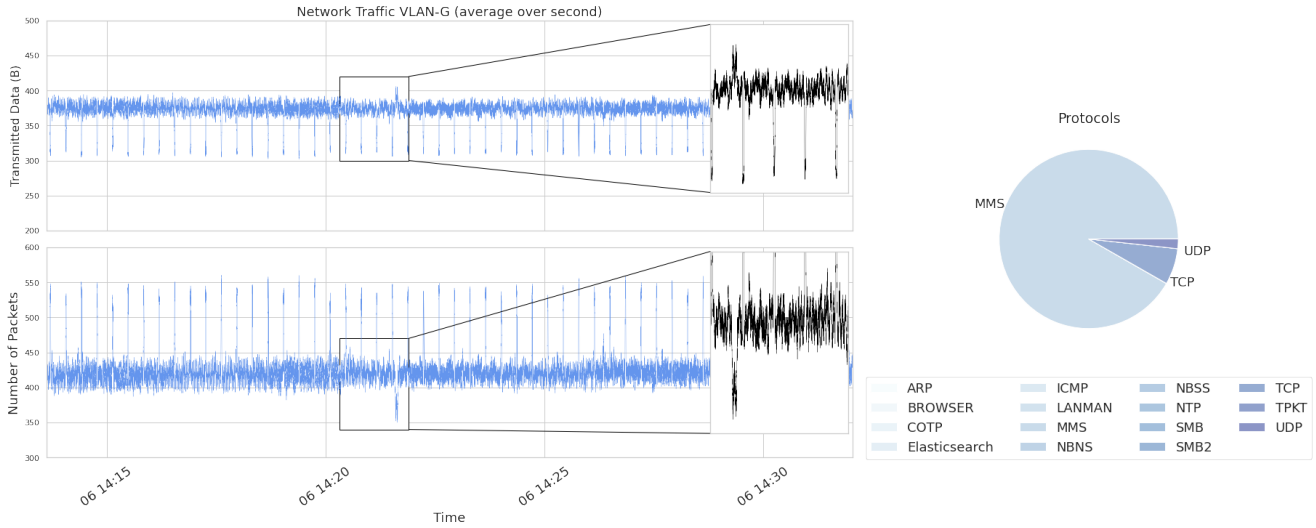

Figure 7. Traffic between AC800Ms and Connectivity Servers in VLAN-G. The pie chart shows the proportion of consumed bandwidth by various communication protocols.

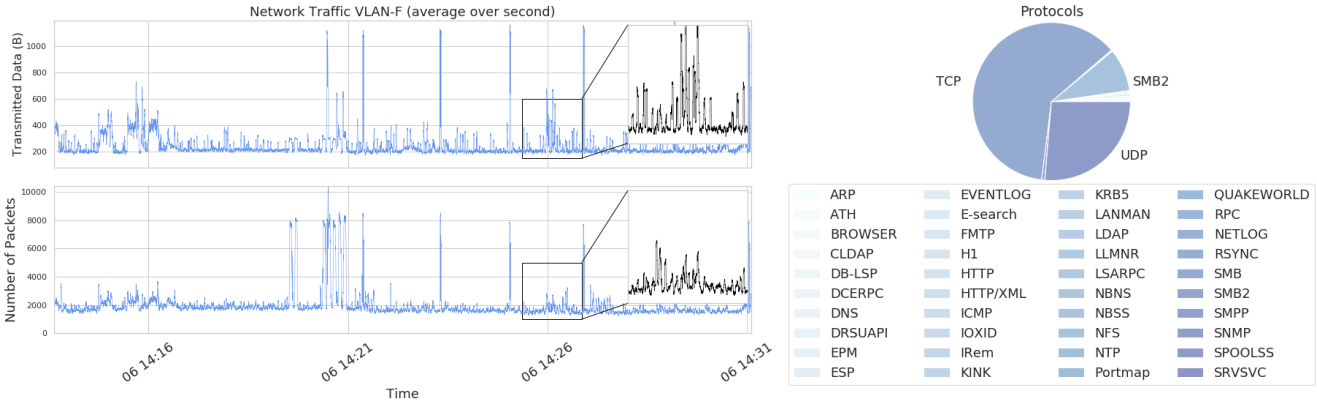

Figure 8. Traffic between the connectivity servers and operator and engineering stations in VLAN-F. The pie chart shows the proportion of consumed bandwidth by various communication protocols.

Knowing about the diversity of OT network traffic, the main challenge would be finding appropriate methods to accommodate OT traffic together with unforeseeable IT network traffic in the same network while still guaranteeing real-time property for process automation applications. The following section will discuss possible technology enablers that aim to achieve such a goal.

3. Technology Enablers for Future Control Architecture

Fundamental technology drivers that make the future industrial network happen are seen in the realization of the three main domains of (i) deterministic communication infrastructure, (ii) edge/fog computing, and (iii) security.

Deterministic communication infrastructures are expected to be addressed according to the Time-Sensitive Networking (TSN) standard, which is under the development of IEEE standardization. TSN is working to provide an innovative networking solution for closed-loop control systems that support mixed traffic in critical applications such as transportation (vehicular/automotive networks, railway, and autonomous cars), motion control, power utility automation, and industrial distributed control systems [8]. Another technology driver is fog/edge computing, which extends cloud computing capabilities in terms of storage, computation, and networking to the edge of the network [9]. Fog computing is the leading architectural enabler supporting low latency, low-power consumption, high reliability, and location awareness that might be of interest in the aforementioned critical applications. Security is another crucial entity that enables future industrial automation. In traditional industrial networks, the main security concern usually correlates to safety definition, where the main goal is to protect humans and machines against the consequences of system failures [10]. By integrating information technology into the industrial control systems, protection against cyberattacks has become the major design goal of Industrial IoT systems [11].

In this paper, we focus on the core functionality of enabling IT traffic in the OT networks. The main challenge is to find means to accommodate an unknown amount of IT traffic while preserving the real-time guarantees for OT traffic in the network. TSN is a developing technology that is expected to have a significant impact on the realization of such functionality while providing a deterministic communication infrastructure. Unfortunately, there is still a lack of corresponding technology candidates for edge/fog computing and security solutions. We believe that when IT and OT convergence is in place, the focus can shift to higher-level functionality and new ways of deploying automation systems for process automation, like edge and cloud solutions. However, history has proven that security cannot easily be retrofitted, and thus, this has to have been taken into account from the start.

3.1. TSN

TSN is a set of IEEE 802 Ethernet substandards that have been developed by the Time-Sensitive Networking task group of the IEEE 802.1 working group [12] with the aim to enable deterministic real-time communication over Ethernet. TSN achieves determinism over Ethernet using a set of tools that can be partitioned into four main domains of (i) time synchronization, (ii) bounded low latency, (iii) ultra reliability, and (iv) resource dedication.

Table 1 lists a number of standards developed in each of these four domains. Time synchronization deals with timing and synchronization; in other words, it provides the network with synchronized clocks. 802.1AS-Rev is the main standard in this domain. The Bounded low latency domain is responsible for the determinism, which guarantees data availability at the expected time by applying different scheduling and forwarding techniques. The Ultrareliability domain targets the reliability of the system, and focuses on the errors, faults, and redundancy techniques to keep the system dependable. The Resource dedication and application programming interface (API) domain enables the high-level planning and configuration required to allow systemwide feature capabilities in heterogeneous networks.

Table 1. A short list of IEEE Time-Sensitive Networking (TSN) Standards. API—application programming interface.

Area of Definition	Standards	Title of Standards
Timing synchronization	802.1AS	Timing and Synchronization
Bounded low latency	802.1Qav	Credit-Based Shaper
	802.1Qbu	Frame Preemption
	802.3br	
	802.1Qbv	Scheduled Traffic Enhancement
	802.1Qch	Cyclic Queuing and Forwarding
	802.1Qcr	Asynchronous Traffic Shaping
Ultrareliability	802.1CB	Frame Replication and Elimination
	802.1Qca	Path Control and Reservation
	802.1Qci	Per-Stream Filtering and Policing
	802.1AS-Rev	Enhancement and performance improvements
Resource dedication and API	802.1Qat	Stream Reservation Protocol
	802.1Qcc	Stream Reservation Protocol/ TSN configuration
	802.1Qcp	YANG Data Model
	802.1CS	Link-local Registration Protocol

The ongoing work on TSN promises hard real-time capabilities. It is also claimed that TSN can reserve the bandwidth exactly according to the application latency requirement and consequently enables the convergence of different networks into one common network that transmits time-sensitive control data together with best-effort data and data with soft real-time requirements. Although this can be seen as a real game-changer for real-time automation applications, it is still unclear how to efficiently select a set of TSN Standards and tune the relevant settings.

In order to derive and develop technical solutions that will enable a transition towards an information-centric architecture, we need to consider how the process industries are established and evolving to stay profitable and competitive. The most obvious scenario that comes to mind is when a brand new production site is built. In this scenario, the automation system providers are competing with their latest and most advanced products and system solutions that solve the site owner's needs. This is referred to as a green-field installation. Another scenario in process automation, probably the most common scenario, where the

company is long-time established with one or more large-scale production sites. Those established companies are most often either modernizing or extending their production capacities or product ranges. In this scenario, there is already a large installed base of automation equipment, as well as existing network infrastructures, in place. This is referred to as a brown-field installation. Based on the two scenarios described above, one can identify the need for a technology migration path in order to achieve the desired market penetration to justify technology investments. In fact, the transition from the de-facto hierarchical system architecture is essential for business and technology success.

Standardization of communication protocols used in hierarchical industrial systems is a critical issue. Today's control systems widely use Profinet and OPC Unified Architecture (OPC UA) to meet the communication requirements of different levels. OPC UA has its strengths in vertical communication between devices of different levels and controller-to-controller communication at the control level. At the same time, Profinet meets all the communication requirements in the field network. Today's network only allows Profinet as the real-time capable protocol (besides TCP/IP-based traffic). TSN will make it possible to converge different communication means by simultaneously running multiple real-time-capable protocols in a single convergent network. The IEC/IEEE 60802 TSN Industry Automation profile proposes flattening of networks so that Profinet and OPC UA to operate on the same network physical layer along with IT data communication such as cloud and video. With TSN integration, the field-level device data and diagnostic information can be collected by controllers from the field network using Profinet over TSN. OPC UA over TSN can deliver the aggregated information to higher-level systems such as ERP, MES and cloud to make informed decisions.

To achieve a flattened network architecture, the network infrastructure needs to cope with the aggregated traffic while preserving the requirement of each traffic flow. As the primary goal of process industries is to produce goods, all the functions are required to operate flawlessly with high availability. If one function fails, the most common scenario is that the process cannot continue to operate. This implies that the requirements and characteristics of different types of traffic flows needs to be studied in relation to other traffic. Furthermore, a high-level classification of various traffic flows can be done by grouping them into different traffic types. The traffic types can then be mapped to network functionality that enables the desired characteristics.

3.2. TSN in the Process Industry

The attempt of standardization of network traffic types is still in progress under the joint IEEE/IEC 60802 standard. Table 2 shows the most developed proposal for traffic classification presented at IEEE/IEC 60802 via the Industrial Internet Consortium, IIC [13]. However, the values for a period, tolerance to loss, and criticality for each traffic type may vary with different applications, which may not strictly follow those listed in Table 2. Mapping various traffic types to TSN mechanisms that fulfill the requirements of each traffic type is also ongoing in IEEE/IEC 60802, with inputs from the Shapers Initiative via Open DeviceNet Vendors Association (ODVA). Table 3 aims to derive the specific TSN mechanisms together with the appropriate recommendation type based on the required QoS level.

As can be seen from Tables 2 and 3 the specification is on its way, but more work is needed to remove ambiguities. For instance, from a process automation perspective, the support for brown-field installations seems to be missing. Moreover, as can be seen from the captured data-set at Iggesund Mill in Section 2, it is far from trivial to map existing communication flows to dedicated TSN mechanisms. It is, by all means, no exercise that is quickly done and requires a lot of domain knowledge in order to derive the correct conclusions. The final performance of TSN networks will heavily depend on the input parameters, and those parameters might be difficult to derive. Assuming several parameters to be derived for each communication flow, the engineering efforts quickly become infeasible and require excellent tool support and engineering guidelines.

Table 2. Traffic types [13] (f: fixed, v: variable).

Types	Periodicity	Period	Synch.	Data Size	Criticality
Isochronous	Periodic	<2 ms	Yes	30–100 B (f)	High
Cyclic	Periodic	2–20 ms	No	50–1000 B (f)	High
Events	Sporadic	n.a.	No	100–1500 B (v)	High
Network Control	Periodic	50 ms–1 s	No	50–500 B (v)	High
Config. and Diag.	Sporadic	n.a.	No	500–1500 B (v)	Medium
Best Effort	Sporadic	n.a.	No	30–1500 B (v)	Low
Video	Periodic	Frame Rate	No	1000–1500 B (v)	Low
Audio and Voice	Periodic	Sampling Rate	No	1000–1500 B (v)	Low

Table 3. Traffic mapping [13]. TC: traffic class, CT: cut-through, RS: reservation scheduling, M: mandatory, O: optional, C: conditional, R: recommended, ^{T}: time-based, ^{R}: rate-based, *: end devices.

Types	802.1Q	TC	802.1Qbv	802.1AS-rev	CT	802.1CB	802.1Qbu	802.1Qci	802.1Qav	RS
Isochronous	M	6	M	M	O	O		M ^{T}		M
Cyclic-Option: Strict Priority	M	5				O	R	M ^{R}		M
Cyclic-Option: Scheduled Traffic	M	5	M	M		O		M ^{R}		M
Events-Control	M	4				O	O	M ^{R}		M
Events, Alarms, and Operator Commands	M	3		M			O	M ^{R}	O *	M
Configuration and Diagnostics	M	2					O	M ^{R}		M
Network Control	M	7			C		C			
Video, Audio, and Voice	M	1					O	M ^{T}	R	M
Best Effort	M	0					O			

4. Evolution Challenges

This section focuses on main evolution challenges including engineering guidelines, tools, security, reliability, and time-synchronization issues and describes the real-time challenges in distributed systems. We also elaborate on possible directions for research in the area of IT/OT convergence.

4.1. Engineering Guidelines

Despite all the benefits TSN promises, it can not be harvested with just a click. For the green-fields, they can adopt TSN in a revolutionary way since they have the largest flexibility to choose from all the available TSN functionalities/devices with a clean slate network including TSN aware end-points. After the traffic analysis, managing all the traffic is another challenge because the legacy end-devices may not support TSN capabilities/management to apply the TSN tools directly. Furthermore, engineers need to derive several parameters, e.g., deadlines, jitter, and packet sizes, to create network schedules, independent of green-field or brown-field installations. With good tool support, the green-field installations can in any case be streamlined compared to the brown-field installations. It takes effort to come up with evolutionary technologies for brown-field networks, and they should be compatible with other TSN technologies that may be deployed in the future. There are also foreseen difficulties from the personnel perspective, especially with the IT and OT staff. With the integration of the IT and OT networks, they are inevitable to interact more often and probably will have disagreements about the responsibility over some new issues emerging in the integrated network (e.g., reserving time slots, tuning maximum burst rates per link, and setting stream identifiers), as well as agreeing on best practices.

4.2. Security Challenges

The transition to more open network architectures, combined with Big Data and Cloud computing, will bring profound opportunities to smart manufacturing systems. At the same time, new security challenges are presented with billions of smart devices interconnected in the world of Industrial IoT. The biggest security concern comes from connecting IoT devices, including sensors, actuators, and edge-computing units, with existing controllers and end devices in automation and manufacturing information networks. These challenges are, of course, on top of applied secure protocols like OPC UA, or the necessity of securing other protocols like Modbus TCP, which are separate essential topics to address.

The existing OT and IT security approaches and policies [14,15] will need to be adapted to embrace these new IoT security challenges. One important direction is the authorization management that assigns the different access levels to only access the necessary data from the OT domain. From the device perspective, smart industrial devices have much smaller footprints of computing power and operating systems. The convention in the traditional automation network assumes that no software or patches are needed once installed, which leaves them to be an important attack surface that is vulnerable to new types of malware or denial of service attacks.

4.3. Engineering Tool Challenges

In TSN, the promised performance relies on traffic engineering and scheduling, which further rely on two TSN entities: (i) Centralized User Configuration (CUC) and (ii) Centralized Network Configuration (CNC), as specified in IEE 802.1 Qcc. CUC is responsible for discovering the network's physical topology, collecting requirements and properties of every TSN flow from the end devices, e.g., the packet size, cycle time, end-to-end latency, and sending the collected information to the CNC. The CNC executes the scheduling and returns the decision of whether a TSN flow can be accepted. For an accepted TSN flow, the corresponding end-to-end path will be sent to CUC together with the scheduling along the path. The scheduling is also sent out from CNC to the bridges along the end-to-end path via network management protocols, e.g., NETCONF.

The first challenge is the lack of a standardized northbound interface of CUC, i.e., the parameters to characterize each TSN flow, which are necessary to reduce the manual input from the operator and enable the plug-and-play functionality of end devices. Another challenge arises from online diagnosis and configuration. After the initial offline scheduling and configuration, the process is expected to operate with very short and even zero downtime. This requires an online diagnosis to detect potential problems beforehand and may further result in some reconfiguration of the related TSN flows. Moreover, online configuration is needed when adding new devices or new applications to the operation network. In this case, CUC will send requests for the new TSN flows to CNC responsible for calculating schedules and updating the configuration. However, when the network is unable to handle new TSN flows due to the lack of available resources, it is not appreciated to simply decline the request and return a notice to upgrade the network. Instead, the CNC should provide a good scheduling strategy to accommodate all the new critical TSN flows while making a negligible effect on the existing TSN flows to limit the configuration changes on the bridges.

From an implementation perspective, the support of YANG models and NETCONF is not entirely in place. Despite the fact that the YANG data model has been included in the TSN standard and it is agreed that NETCONF will serve as the network management protocol between CNC and the bridges, the development of YANG models and NETCONF in many switches progress rather slow compared to other TSN functionalities. The lack of efficient configuration presents a gap to enable an automated engineering workflow.

4.4. Reliability Challenges

Providing a reliable system is essential for any type of network, and TSN is not an exception. Implementing fault-tolerance solutions is one of the major steps towards system reliability, which is mainly addressed through redundancy mechanisms. In TSN, fault tolerance can be achieved through two main substandards: (i) path control and reservation (IEEE 802.1Qca) that enable the creation of multiple paths in the network; (ii) frame replication and elimination (IEEE 802.1CB) that allow replication of streams and deploying them through the paths created by the Qca substandard—see Table 1. However, the way that those aforementioned mechanisms are set is very dependent on the application requirements [16]. One setting, called the decoupled approach, allows for arbitrary redundancy protocols to be utilized by decoupling the stream reservation from the redundancy mechanism. This setting is more appropriate for applications that have less stringent reliability

requirements. Another setting, called harmonized, integrates the establishment of the reservation and the redundancy requirements at the cost of higher protocol overhead and bandwidth demands.

Another important aspect of process automation systems is that a single point of error must be avoided in many scenarios. In order to meet that requirement, the end-nodes themselves need to be redundant. From a network perspective, this means that there are two independent network ports on the devices, which are required to be connected to two different switches to avoid a single point of error. In this perspective, the IEEE 802.1CB and IEEE 802.1Qca standards are not sufficient as they only provide network redundancy and not end-to-end redundancy. Moreover, an IEEE 802.1Qca update is needed to associate dual network ports of the redundant end-points.

4.5. Distributed Real-Time System Challenges

Distributed real-time systems are commonly deployed in process automation, where the whole process is carried out with multiple control networks, each consisting of a local set of sensors and actuators [17]. The process conditions are monitored periodically by the sensors, which can be denoted as a snapshot of the whole process line. The controllers are responsible for making computations based on the received snapshot and sending out action commands to the actuators within predefined time bounds. To guarantee correct operation, the periodic process snapshot, as well as the functionality of all the controllers, should be available at every controller that needs the data before executing the control application. For instance, all the controllers belonging to the distributed control system need to act on the same set of information in order to guarantee the correct output. This is a general requirement that the system should be in a consistent state at all times, independent of if there are changes in process data, applications, or in the network. Changes have to be coordinated in time as well in order to preserve the real-time properties during run-time changes and avoid bringing the ongoing process down.

4.6. Synchronization

Synchronization of industrial devices and systems with adequate accuracy and precision is an essential part of monitoring and control functions of automation systems. Different synchronization requirements per application, harsh environment, and nondeterministic networks make the synchronization in industrial systems challenging.

With TSN, the IEEE802.1AS standard is introduced. The revision of this standard, IEEE802.1AS-rev, is under discussion. It is envisioned to provide fault tolerance and highly accurate time synchronization. The green-field installations would get benefited by implementing this feature-rich synchronization profile. However, the comprehensive functional and security performance of a new profile in the industrial environment has yet to be assessed.

In the case of brown-field installations, the automation systems typically require one to a few thousands of milliseconds of synchronization accuracy for most of their applications. Since the TSN networks operate at the synchronization accuracy of nanoseconds order, integrating legacy industrial devices to the TSN network and thereby achieving deterministic data delivery of critical messages is technically challenging.

5. Research Directions

Among the discussed challenges above, the engineering guideline for brown-field is the most important research question since it is the base for all the other functionalities to build upon. Though each brown-field site also varies from each other in terms of applications and end devices, it is adequate to derive guidelines with basic functionality to achieve IT/OT integration in process automation together with the flexibility to tune parameters in each site. An important aspect of the guidelines is to address engineering of the network performance, i.e., performance analysis models and diagnosis methods for the design of a scalable and reliable network that can detect errors and identify bot-

tlenecks. This process requires broad knowledge about the various services and traffics accommodated in the IT/OT network by learning their relevant parameters and important Key Performance Indicators (KPIs). The direct challenge here would be that a green-field that can evolve and adapt various TSN methods does not have any initial traffic to be investigated. Therefore, studying brown-field traffic is the closest path to understand the required performance criteria for various traffic types to provide the network performance engineering guidelines of IT/OT networks. Along with the guidelines design, security issues and solutions should come along, as the network structure and functionalities affect the security performance and the security solutions in turn affect the network performance. Another important research topic is the engineering tool, which is the key to bootstrap the system and maintain smooth operation during the production phase. Reliability is also important for control networks, and single-point failure protection should be considered besides network redundancy. For the cases that require distributed real-time systems, both configuration and synchronization are also essential, and distributed real-time system configuration requires more domain expertise besides general solutions.

Related Works

As discussed earlier, modeling network traffic to identify network structure and data flow characteristics can be seen as a prerequisite of network evolution. In this regard, there exist many research works in the IoT domain, many notably considered intrusion and anomaly detection [18–23], but very few have focused on the profiling network traffic of industrial networks. Authors in [20] introduce communication models of various industrial networks based on traffic profiling by applying probabilistic modeling on network traffic, considering both periodic and aperiodic communication. However, the complexity of the model demands a new round of learning with any configuration changes. Markov chain model is employed in [19] to learn the regularity of packet flows by considering each packet as a state.

An anomaly-based intrusion detection system that uses fuzzy logic to assess whether malicious activity is taking place on a network is presented in [23]. The system consists of a network data collector that reads raw network packets and stores them on a disk. A network data processor then performs data mining on the collected packets, and finally, the observed value is used as an input to the fuzzy analyzer.

Many research papers have reviewed different aspects of IEEE TSN standards [24–26]. A comprehensive survey of queuing and scheduling mechanisms for supporting large-scale deterministic networks was discussed in [25], followed by the most recent research work [26] that presents a comprehensive survey of TSN standards and research studies addressing networking mechanisms for ultra-low-latency applications, such as in industrial control. Instead, the authors in [24] provide an extensive overview of the different fault-resilience concepts for IEEE 802.1 TSN networks.

Many research works have been conducted targeting a specific feature of IEEE TSN standards, including fault tolerance [27–29], traffic planning and shaping [30–33], and time synchronization [26,34]. However, it is important to mention that in this section, we only highlighted some selected references and did not intend to present an exhaustive survey of the broad and vast TSN research domain.

6. Conclusions

There is an increasing need to bridge the gap between the IT and OT networks in the process industry to take the next leap in productivity and innovation. Our case study at a typical process automation factory is a first step to provide the characteristics of OT traffic and aims to inspire more research and standardization work towards the IT/OT convergence for process automation. Due to the variety of process automation scenarios as well as the underlying network topology, applications, and communication protocols used, more case studies should be taken to reveal the comprehensive traffic characteristics in process automation. TSN is one promising technology towards collapsing the networks.

However, in order to deploy TSN in large-scale production facilities, many challenges need to be addressed beforehand. Specifically, further research in the areas of efficient engineering, security, automatic tool support, traffic modeling and profiling, and online monitoring are necessary. Moreover, it is crucial to preserve the performance and characteristics of the distributed real-time systems that are required for process automation. We appeal for more research efforts on deriving engineering guidelines for brown-field, including network performance analysis, as it is the base upon which to add other functionalities and eventually integrate IT and OT systems.

Author Contributions: Conceptualization, all authors; investigation, all authors; writing—original draft preparation and review and editing, all authors; visualization, M.L. and X.J.; funding acquisition, J.Å., J.F.Å., M.B., and T.L. All authors have read and agreed to the published version of the manuscript.

Funding: This work has been partly financed by the Future Industrial Networks (FIN) project, grant number 2018-02196, and Post-FIN project, grant number 2019-02697, within the strategic innovation program for process industrial IT and automation, PiiA, and PiiA Research Etapp II, a joint program by Vinnova, Formas and Energimyndigheten.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data is available upon request from the reviewers.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Bader, S.R.; Maleshkova, M.; Lohmann, S. Structuring Reference Architectures for the Industrial Internet of Things. *Future Internet* **2019**, *11*, 151. [CrossRef]
2. Trunzer, E.; Calà, A.; Leitão, P.; Gepp, M.; Kinghorst, J.; Lüder, A.; Schauerte, H.; Reifferscheid, M.; Vogel-Heuser, B. System architectures for Industrie 4.0 applications. *Prod. Eng.* **2019**, *13*, 247–257. [CrossRef]
3. Colombo, A.W.; Karnouskos, S.; Kaynak, O.; Shi, Y.; Yin, S. Industrial cyberphysical systems: A backbone of the fourth industrial revolution. *IEEE Ind. Electron. Mag.* **2017**, *11*, 6–16. [CrossRef]
4. Wollschlaeger, M.; Sauter, T.; Jasperneite, J. The future of industrial communication: Automation networks in the era of the internet of things and industry 4.0. *IEEE Ind. Electron. Mag.* **2017**, *11*, 17–27. [CrossRef]
5. González, I.; Calderón, A.J.; Figueiredo, J.; Sousa, J. A literature survey on open platform communications (OPC) applied to advanced industrial environments. *Electronics* **2019**, *8*, 510. [CrossRef]
6. Givehchi, O.; Landsdorf, K.; Simoens, P.; Colombo, A.W. Interoperability for industrial cyber-physical systems: An approach for legacy systems. *IEEE Trans. Ind. Inform.* **2017**, *13*, 3370–3378. [CrossRef]
7. Lu,Y.; Riddick, F.; Ivezic, N. The paradigm shift in smart manufacturing system architecture. In *IFIP Advances in Information and Communication Technology, Proceedings of the IFIP International Conference on Advances in Production Management Systems, Iguassu Falls, Brazil, 3–7 September 2016*; Springer: Cham, Switzerland, 2016; pp. 767–776.
8. Ditzel, G.A.; Didier, P. Time sensitive network (TSN) protocols and use in Ethernet/IP systems. In Proceedings of the ODVA Industry Conference & 17th Annual Meeting, Nuremberg, Germany, 15 October 2015; pp. 1–24.
9. Bonomi, F.; Milito, R.; Zhu, J.; Addepalli, S. Fog computing and its role in the internet of things. In Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing, Helsinki, Finland, 13–17 August 2012; pp. 13–16.
10. Zhao, K.; Ge, L. A survey on the internet of things security. In Proceedings of the 2013 Ninth International Conference on Computational Intelligence and Security, Leshan, China, 14–15 December 2013; pp. 663–667.
11. Sadeghi, A.R.; Wachsmann, C.; Waidner, M. Security and privacy challenges in industrial internet of things. In Proceedings of the 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), San Francisco, CA, USA, 8–12 June 2015; pp. 1–6.
12. Time-Sensitive Networking Task Group. Available online: https://www.ieee802.org/1/pages/tsn.html (accessed on 25 March 2021).
13. Industrial Internet Consortium. Time Sensitive Networks for Flexible Manufacturing Testbed Characterization and Mapping of Converged Traffic Types. Available online: https://www.iiconsortium.org/pdf (accessed on 25 March 2021).
14. Knapp, E.D.; Langill, J.T. *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*; Syngress: Burlington, MA, USA, 2014.
15. IEC. *International Electrotechnical Commission, Industrial Communication Networks—Network and System Security—Part 1-1: Terminology, Concepts and Models, IEC/TS 62443-1-1 ed1.0*; IEC: Geneva, Switzerland, 2009.
16. Kleineberg, O.; Fröhlich, P.; Heffernan, D. Fault-tolerant audio and video bridging (AVB) ethernet: A novel method for redundant stream registration configuration. In Proceedings of the 2012 IEEE 17th International Conference on Emerging Technologies & Factory Automation. Krakow, Poland, 17–21 September 2012; pp. 1–8.
17. Erciyes, K. Distributed real-time systems. In *Distributed Real-Time Systems*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 41–62.

18. Weissenberg, M.; Głąbowski, M.; Hanczewski, S.; Stasiak, M.; Zwierzykowski, P.; Bai, V. Traffic Modeling in Industrial Ethernet Networks. *Int. J. Electron. Telecommun.* **2020**, *66*, 145–153.
19. Tamura, K.; Matsuura, K. Improvement of anomaly detection performance using packet flow regularity in industrial control networks. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **2019**, *102*, 65–73. [CrossRef]
20. Faisal, M.A.; Cardenas, A.A.; Wool, A. Profiling communications in industrial IP networks: Model complexity and anomaly detection. In *Security and Privacy Trends in the Industrial Internet of Things*; Alcaraz, C., Ed.; Springer: Cham, Switzerland, 2019; pp. 139–160.
21. Sheng, C.; Yao, Y.; Yang, W.; Liu, Y.; Fu, Q. How to fingerprint attack traffic against industrial control system network. In Proceedings of the 2019 1st International Conference on Industrial Artificial Intelligence (IAI), Shenyang, China, 23–27 July 2019; pp. 1–6.
22. Mahmoud, M.S.; Hamdan, M.M.; Baroudi, U.A. Modeling and control of cyber-physical systems subject to cyber attacks: A survey of recent advances and challenges. *Neurocomputing* **2019**, *10*, 101–115. [CrossRef]
23. Dickerson, J.E.; Dickerson, J.A. Fuzzy network profiling for intrusion detection. In Proceedings of the 19th International Conference of the North American Fuzzy Information Processing Society (NAFIPS), Atlanta, GA, USA, 13–15 July 2000; pp. 301–306.
24. Kehrer, S.; Kleineberg, O.; Heffernan, D. A comparison of fault-tolerance concepts for IEEE 802.1 Time Sensitive Networks (TSN). In Proceedings of the 2014 IEEE Emerging Technology and Factory Automation (ETFA), Barcelona, Spain, 16–19 September 2014; pp. 1–8.
25. Nasrallah, A.; Balasubramanian, V.; Thyagaturu, A.; Reisslein, M.; ElBakoury, H. TSN algorithms for large scale networks: A survey and conceptual comparison. *arXiv* **2019**, arXiv:1905.08478.
26. Nasrallah, A.; Thyagaturu, A.S.; Alharbi, Z.; Wang, C.; Shao, X.; Reisslein, M.; ElBakoury, H. Ultra-low latency (ULL) networks: The IEEE TSN and IETF DetNet standards and related 5G ULL research. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 88–145. [CrossRef]
27. Gavrilut, V.; Zarrin, B.; Pop, P.; Samii, S. Fault-tolerant topology and routing synthesis for IEEE time-sensitive networking. In Proceedings of the 25th International Conference on Real-Time Networks and Systems, Grenoble, France, 4–6 October 2017; Association for Computing Machinery: New York, NY, USA, 2017; pp. 267–276.
28. Atallah, A.A.; Hamad, G.B.; Mohamed, O.A. Fault-Resilient Topology Planning and Traffic Configuration for IEEE 802.1Qbv TSN Networks. In Proceedings of the IEEE 24th International Symposium on On-Line Testing and Robust System Design (IOLTS), Platja d'Aro, Spain, 2–4 July 2018; pp. 151–156.
29. Alvarez, I.; Proenza, J.; Barranco, M.; Knezic, M. Towards a time redundancy mechanism for critical frames in time-sensitive networking. In Proceedings of the 2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Limassol, Cyprus, 12–15 September 2017; pp. 1–4.
30. Steiner, W.; Craciunas, S.S.; Oliver, R.S. Traffic Planning for Time-Sensitive Communication. *IEEE Commun. Stand. Mag.* **2018**, *2*, 42–47. [CrossRef]
31. Dos Santos, A.C.T.; Schneider, B.; Nigam, V. TSNSCHED: Automated Schedule Generation for Time Sensitive Networking. In Proceedings of the 2019 Formal Methods in Computer Aided Design (FMCAD), San Jose, CA, USA, 22–25 October 2019; pp. 69–77.
32. Atallah, A.A.; Hamad, G.B.; Mohamed, O.A. Routing and Scheduling of Time-Triggered Traffic in Time-Sensitive Networks. *IEEE Trans. Ind. Inform.* **2019**, *16*, 4525–4534. [CrossRef]
33. Nayak, N.G. Scheduling & Routing Time-Triggered Traffic in Time-Sensitive Networks. Ph.D. Thesis, University of Stuttgart, Stuttgart, Germany, 8 November 2018.
34. Steiner, W. Interoperability of IEEE 802.1 AS and Fault-Tolerant Clock Synchronization. Presentation on IEEE 802. Available online: http://www.ieee802.org/1/files/public/docs2013/ (accessed on 25 March 2021).