Tableau: Future-Proof Zoning for OT Networks

Piet De Vaere[1], Claude Hähni[1], Franco Monti[2], and Adrian Perrig[1]

[1] ETH Zürich, Switzerland
{piet.de.vaere, claude.haehni, adrian.perrig}@inf.ethz.ch
[2] Monti Stampa Furrer & Partners AG
franco.monti@msfpartners.com

Abstract. For over two decades, hierarchical zoning models have dominated operational technology (OT) network design. However, ongoing changes to industrial network technologies and workloads, together with rising threat levels, are now challenging this design pattern. To address these issues, this paper introduces Tableau, a new zoning architecture for OT networks. Tableau increases network flexibility by flattening the zone structure and by allowing the seamless integration of plant, edge, corporate, and cloud networks. Simultaneously, Tableau facilitates modern security practices and is IEC 62443 compatible, ensuring the continued secure operation of OT infrastructure.

Keywords: OT networking · Network zoning · Industrial IoT

1 Introduction

Since the introduction of computerized control systems to industrial automation, operational technology (OT) networks have had a strong hierarchical structure. One of the most prominent drivers behind this design is the Purdue Reference Model [4,26], which is widely considered to be the gold standard for designing and securing OT networks; especially in critical infrastructures such as utilities.

More broadly, the hierarchical structure of OT networks has historically been motivated by two reasons. First, industrial processes tend to exhibit natural hierarchy, as is commonly illustrated using the automation pyramid (see Section 2). Because control systems are usually placed close to the processes they control, it is natural for them to inherit the hierarchical structure of these processes. Second, using a hierarchical structure allows network designers to place security checkpoints between network levels, incrementally increasing the security level as the hierarchy descends.

For over two decades, OT network designers have successfully followed this approach. However, in recent years, the relevance of the hierarchical model is increasingly being questioned, as the model is struggling to adapt to new realities in the automation space [6,7,12,17,18,25], and because of the increasing convergence between information technology (IT) and OT systems. In most networks, network designers already had to give up the strict air gap between IT and OT infrastructure in order to support remote management of automation

systems, and new trends are further challenging the hierarchical model. Concretely, these trends can be classified as changes (i) to the network, (ii) to the the automation infrastructure, (iii) to information flows, (iv) to threat models, and (v) to operation models. For example, cloud-based predictive maintenance requires raw information to flow directly from sensors on the lowest levels of the network to the cloud, crossing all traditional network levels. This contradicts the hierarchical design principle that individual network flows should not cross more than one network level at once. We further discuss the challenges created by new OT trends in Section 3.

Even though the trends introduced above do not render the current network model unusable, they do render it increasingly impractical. Even worse, they incrementally erode the security properties of hierarchical network design. Therefore, it is time to reconsider how we organize OT networks by introducing modern network management techniques to the OT environment. This will allow us to satisfy the contemporary demands placed on our networks, while achieving a high level of security.

To that end, this paper introduces Tableau, a modern zoning model for OT networks. Tableau builds on Mondrian [13], a recently developed zoning architecture for IT networks (see Section 4), and makes it suitable for operation on OT networks by defining a new Mondrian deployment model. By doing so, Tableau enables highly flexible network management in OT settings. Particularly, Tableau facilitates the seamless and secure integration of networked resources on the plant floor, at the edge, in the corporate network, and even in the cloud. Moreover, Tableau makes supplier access to OT infrastructures such as PLC, SCADA or HMI systems easier to configure, and reduces the impact of supply chain attacks by facilitating the creation of more, and smaller, network zones. In addition, Tableau accomplishes all of this while remaining compatible with IEC 62443, the leading standard for security in industrial networks [11].

Because of the large number of legacy systems typically present in OT networks, Tableau was designed to be brownfield-compatible. Concretely, Tableau provides the following two backward compatibility properties. First, Tableau can be incrementally deployed on subsections of the network while maintaining full network functionality. Second, it is possible to instantiate a hierarchical network structure on top of a Tableau network. Doing so enables network operators to gradually transition their network policies from the hierarchical to the Tableau model. We present the Tableau zoning architecture in Section 5, and we illustrate its features using examples based on a typical critical infrastructure network.

Tableau represents a significant break from the established, hierarchy-based security mindset in OT networks. We discuss the implications of this change in Section 6. Concretely, we argue that (i) by leveraging modern security mechanisms, and (ii) considering the changes that have occurred to OT networks since the hierarchical security models were established, Tableau not only provides much more flexibility to network administrators, but also *increases* the security of the networks in which it is deployed.

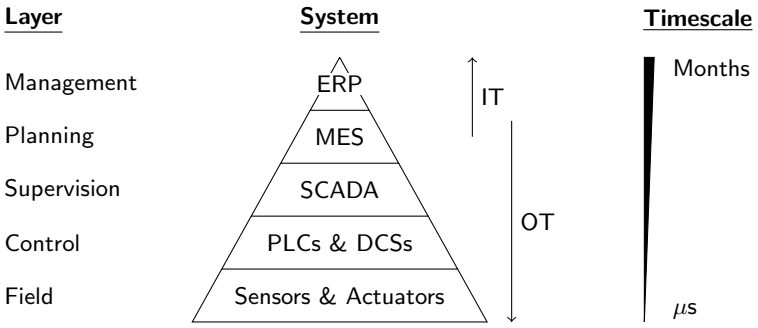


Fig. 1: The automation pyramid.

2 Current OT Networks

Industrial processes are often modeled using the automation pyramid [22]. This model, shown in Figure 1, is used to capture the hierarchical structure found in industrial organizations, and applies to a broad range of industries. The lowest level of the automation pyramid contains the systems that directly interact with the physical processes that are controlled, i.e., sensors and actuators. Traversing the pyramid upwards, each consecutive level adds a layer of abstraction and aggregation until finally the top level, containing the organization's management, is reached. Two common observations can be made throughout the pyramid. First, process feedback always flows upwards between the levels, while commands flow downwards; there is no direct lateral information flow. Second, the further the distance from the process, the larger the decision timescales become. Traditionally, the lower levels of the automation pyramid are part of the OT network, and the top part of the IT network, but, as we discuss in Section 3, this line is blurring.

For communication networks, the hierarchical structure of the automation pyramid is translated to what is commonly referred to as a *Purdue Network*, referencing the *Purdue Model for Control Hierarchy* [26]. We illustrate a Purdue Model-based network in Figure 2, which shows a network as would typically be found in critical infrastructure. In a Purdue network, network zones are organized in hierarchical levels. Further, zones are organized in such a way that all communication between zones on the same level must traverse a zone of a higher level, and firewalls enforce security policies at each zone transition. For technical reasons, communication on the lowest Purdue layers usually use specialized *fieldbus* networks, further segregating devices deployed in the field from higher layers.

The principal ideas behind this network architecture are that (i) each lower network level has stronger security properties than the one above it, and that (ii) an attacker needs to breach many security boundaries before being able to access the organization's most critical assets (i.e., obtain control over the physical processes). In order for these properties to hold, it is important to design network flows to cross as few zone boundaries as possible. After all, each

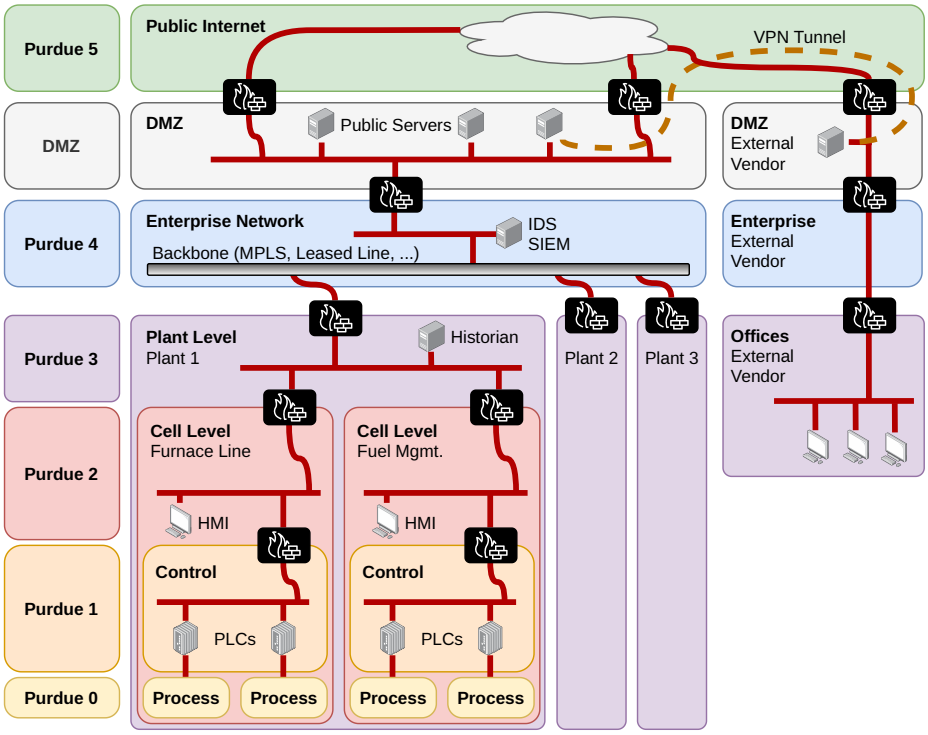


Fig. 2: A typical Purdue Model-based network.

permitted network flow can be used as a conduit for an attack. Thus, if a single flow crosses multiple security boundaries at once, an attacker can use this flow to bypass Purdue levels.

3 Challenges to OT Networks

The Purdue-based network design discussed in Section 2 has successfully served OT operators for over two decades. However, with the advent of the Industrial Internet of Things (IIoT) and the "fourth industrial revolution", the requirements placed on the network are rapidly changing, putting pressure on the Purdue design. We discuss the most significant drivers for these changes in this section.

Changes to the network. In the last decade, software-defined networking (SDN) has transformed how IT networks are being operated. So far this change has not yet significantly affected OT networks, but the ongoing convergence of IT and OT systems [3] suggests that it is only a matter of time before this will change. Moreover, recent work from the IEEE Time-Sensitive Networking (TSN) working group [8], including the specification of a TSN profile for industrial automation [9], will allow even the lowest levels of automation networks to use standard Ethernet [15,27]. This will likely lead to a replacement of the current fieldbus

protocols, and will more closely integrate field devices with higher levels of the automation system, in turn making it harder to maintain the strict separation of Purdue levels and easier for an attacker to cross from the higher levels to secondary technologies deployed in the lower levels.

Further, new networking technologies, such as TSN and SDN, are increasingly centrally managed, which decreases both the relevance and robustness of distributed security enforcement. For example, when an SDN controller is compromised, the adversary can redefine the network fabric to route packets around firewalls, effectively disabling them [23].

Evolution of the automation infrastructure. It is common that as the technological capabilities of a system start to exceed the requirements placed on that system by its users, more and more components of that system are replaced by general-purpose components. We have clearly witnessed this in the data center industry with the advent of virtualization technologies (both for end-hosts and for network functions), and also IT/OT convergence is a manifestation of this phenomenon.

Another manifestation of this phenomenon is the rise of *virtualized automation functions*, such as soft-PLC, soft-SCADA, and soft-HMI systems. Contrary to their physical counterparts, virtualized automation functions do not need to be placed physically close to the processes they control. New network technologies (such as TSN) facilitate this further. Concretely, these virtualized computation resources can be placed at the edge (for functions in lower levels of the automation pyramid), or even in the cloud (for functions in the middle to higher levels of the pyramid). This is problematic as current industrial networks are not designed to place physically distant devices logically nearby in the network.

Changes to information flows. In traditional automation networks, information does not travel across more than one level of the Purdue Model without being proxied or aggregated. However, the advent of cloud-based big-data analytics for applications such as predictive maintenance has disrupted this. In order to obtain the most accurate predictions, as much raw data from the lower levels of the automation pyramid as possible is now being collected and directly uploaded to the cloud. Supporting such data flows in current networks leads to high management overhead and violates the security principles of the Purdue Model.

Changes to threat models. The security of the Purdue Model is primarily based on the assumption that attackers enter the network at the top levels of the model, and have to work their way down into the lower levels with higher security. However, (i) the increased number of network flows that cross multiple Purdue levels at once, (ii) the increased complexity—and thus vulnerability—of automation devices, and (iii) the increased use of wireless and portable technologies are making it increasingly more likely for an attacker to enter the network directly at a lower Purdue level. This breaks the assumption that the security

level of the network increases as one descends through the levels of the Purdue Model.

Changes in the industrial target operation model. Cost pressure and operational efficiency are leading to the regional cluster model, in which several geographically dispersed plants are remotely managed from a single regional node plant. This allows companies to reduce the personnel required to run plants, and to increase remote operations, sometimes even cross-border. However, such a topology of plants, besides building on an increased level of digitalization, adds complexity into the overall configuration when a Purdue-based configuration is maintained. Moreover, traffic flows between a regional node plant and its cluster plants might traverse public networks. This exposes the traffic to man-in-the-middle and spoofing attacks, which in turn can lead to a loss of control over the remotely managed plants. Hence, additional measures need to be taken to assure the integrity and availability of industrial traffic flows.

4 Mondrian Network Zoning

Mondrian [13] is a recent zoning architecture for enterprise networks that was motivated by the need for modern network models which is arising in cloud and hybrid-cloud deployments. These new deployment scenarios are posing additional demands on IT security in large corporate networks. Traditionally, information was processed within a single domain. Today, IT infrastructures are distributed across several heterogeneous systems that all need to communicate with each other. This has lead to increased complexity in the structure of IT networks, with a myriad of systems and policies that need to be managed, kept synchronized, and kept consistent. This is similar to what we are currently experiencing in OT networks. Mondrian offers a secure, flexible, and scalable network zoning architecture that alleviates these issues. One notable property of Mondrian is its capability to securely bridge geographically distributed, heterogeneous networks over untrusted infrastructure. As a result, Mondrian opens the door for many interesting deployment scenarios in which a highly secure and easy to manage zoning architecture is required. In this section, we provide a brief introduction to Mondrian and highlight the properties relevant for Tableau.

4.1 Mondrian Overview

Network Zoning with Mondrian. In contrast to current, highly-complex organization of network zones, Mondrian partitions the network into a collection of flat zones. As illustrated in Figure 3, each of these zones is connected to a designated security gateway called the transition point (TP). Placing zones adjacent to each other, only separated by the TP, simplifies today's network architectures in which traffic often needs to traverse multiple layers to reach its destination. A logically centralized controller provides a comprehensive management interface

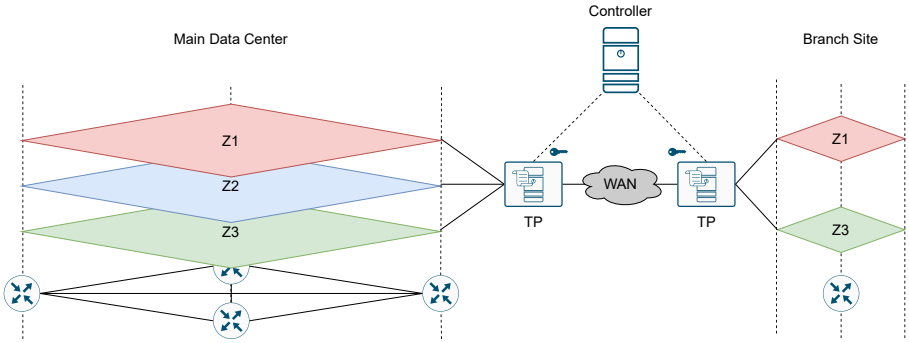


Fig. 3: Mondrian architecture overview. The TPs deployed at each site span the inter-domain transit zone across the wide area network (WAN). The central controller periodically distributes policy updates to the TPs at each branch site. TPs enforce the zone transition policy received from the controller by filtering packets at the local network perimeter. The same logical zone can be distributed across different branch sites (e.g., zones Z1 and Z3).

for operators to orchestrate the network. Common tasks, such as zone migration and zone initialization become much easier, as the network configuration is centralized on a single system. TPs ensure source authentication, zone access authorization, and ingress/egress filtering for all connected network zones. Using the concept of an *inter-domain transit zone*, Mondrian enables network zoning across the boundaries of local networks. This is particularly useful for enterprises that operate geographically distributed branch sites or leverage the cloud as part of their infrastructure.

Flexibility and Scalability. The brain of Mondrian is the logically centralized controller, presenting a single interface with which network operators manage their network. Sites, zones and transition policies can all be centrally managed through this interface. The controller then takes care of distributing these policies to the TPs, which enforce the policies at the individual premises.

Supporting fine-grained zone transition policies offers great flexibility for operators to cover a diverse set of use cases. The centralized interface simplifies today's complex infrastructure with potentially many systems and their respective configurations that need to be updated for every change to the network. As a result, Mondrian is less susceptible to configuration errors and makes policy reviews more efficient. In concert, these properties significantly enhance management scalability.

Deployability. Mondrian supports multiple deployment methods that can be used in conjunction with each other. The primary method uses TPs in the form of all-in-one gateways which perform routing, packet authorization, and tunneling, all without requiring any changes to end hosts. This method reduces the number of security middleboxes that need to be maintained in networks. When using

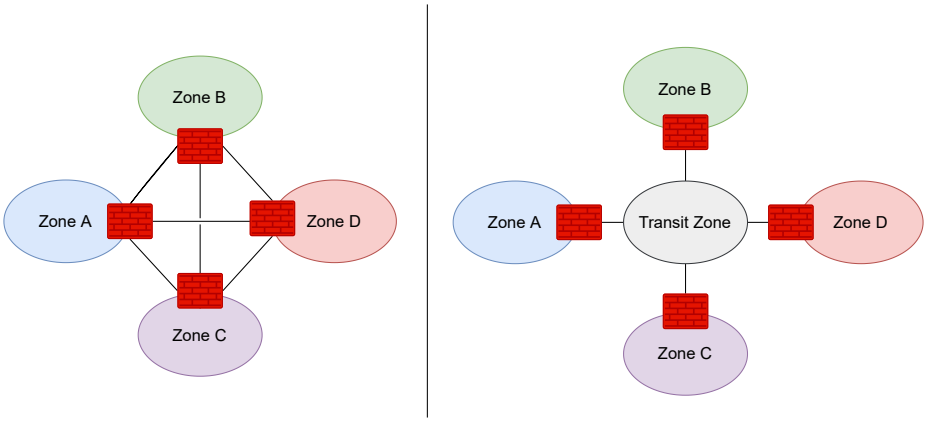


Fig. 4: On the left: a network topology using dedicated links to connect each pair of zones. On the right: The same network organized in a hub-spoke configuration using a transit zone as central element.

this method, Mondrian can also assume a supportive role in which traffic is pre-filtered before it gets handled by security middleboxes.

Alternatively, Mondrian can be deployed purely in software on commodity computing devices. Similar to a VPN, this allows individuals to remotely access network assets from their personal devices in a secure and authenticated manner. When using this method, a TP runs as virtual gateway on a computer and tunnels packets from the device to a remote TP in the enterprise. In contrast to a traditional VPN, a software TP is part of the regular Mondrian deployment and seamlessly integrates with the rest of the architecture.

4.2 Mondrian in Detail

Inter-domain transit zone. One of the main building blocks that allows Mondrian to achieve the properties introduced above is the concept of the inter-domain transit zone. Transit zones are commonly used within local networks to facilitate zone transitions. Concretely, they are special zones that do not contain any end hosts, but merely exist to interconnect other zones. Put differently, a transit zone is the hub in a hub-spoke network topology, providing connectivity between all the other zones. Hub-spoke configurations allow physically separated network zones to access shared services without the need for dedicated links between each pair of zones (see Figure 4). Mondrian scales transit zones to inter-domain networks. The inter-domain transit zone spans across a WAN, connecting the branch sites of enterprises. At every site, local zones are directly attached to the inter-domain transit zone, thus creating a collection of disjoint, parallel network zones. Such a network requires packets to traverse fewer security middleboxes as all zone transitions can be checked already at the border of the inter-domain transit zone. Inside the transit zone, the Mondrian protocol is used to transport zone information across the inter-domain transit zone, allowing remote desti-

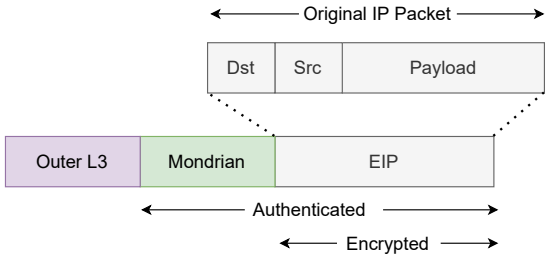


Fig. 5: A depiction of the Mondrian encapsulation. For packets traversing the inter-domain transit zone, a Mondrian header including a zone authenticator is attached to the encrypted original IP packet (EIP). Finally, the Mondrian packet is wrapped in an outer Layer-3 header.

nations to easily verify zone transitions, even if the the underlying network is untrusted. Additionally, the Mondrian protocol is independent from the internal protocols used at each site, which means it is able to bridge networks that operate on otherwise incompatible internal protocols.

Transition points & controller. At each network site, Mondrian deploys a dedicated security gateway, called the transition point (TP). Network zones (subnets) at every branch site are directly connected to the TP, creating a flat network structure (see Figure 3). This means that all inter-zone traffic needs to pass at least one TP. Together, TPs span the inter-domain transit zone. The main task of a TP is twofold: (i) it ensures that traffic does not violate the zone transition policy. For that, TPs check all zone transitions against a policy they receive from a logically centralized controller. On an abstract level, this transition policy is a matrix which defines for each ordered pair of zones (A, B) which traffic is allowed to flow from zone A to zone B. The controller has the full view over the entire distributed network and makes sure that all sites operate with the latest security policy. (ii) For zone transitions that cross the inter-domain transit zone, the second task of TPs is to attach cryptographically secured zone information to each packet before encrypting and forwarding the packet over the WAN. This way, Mondrian achieves integrity and confidentiality of information being sent over a potentially untrusted network. Because the complete original packet, including headers, is encrypted, internal addresses are prevented from leaking. Upon receiving a packet, the remote TP can verify the zone information, decrypt the packet and, if all checks succeed, forward the packet into the local network. The latency overhead introduced by each TP is less than 5 μS [13].

Packet life-cycle. The life-cycle of a packet in a Mondrian network is as follows.

1. An end host in a source zone Z_S sends an IP packet towards an end host in a destination zone Z_D by creating a regular IP packet with the usual source and destination addresses.
   (a) If $Z_S = Z_D$, the packet is delivered directly by the Layer-2 protocol.

   (b) Otherwise, the packet needs to be forwarded via a Mondrian TP.
2. The TP analyzes the packet, retrieving Z_S and Z_D based on the source and destination address of the packet, ensuring that the zone transition Z_S to Z_D is allowed.
   (a) If not, the packet is dropped.
   (b) If yes, the packet is forwarded towards the destination.
3. Next, based on the destination address, the TP evaluates if the packet is destined for an end host in the same branch site.
   (a) If yes, the TP forwards the packet towards the destination in the internal network.
   (b) In case the destination is in a different network across the inter-domain transit zone, the TP looks up the remote TP, creates a cryptoghraphic authenticator, encrypts the original IP packet, and encapsulates the encrypted packet together with the Mondrian header in an outer Layer 3 header (see Figure 5). The exact outer layer depends on the protocol used within the inter-domain transit zone. This packet is then forwarded to the remote TP.
4. Finally, the receiving TP decapsulates the payload, verifies the authenticator and, if all checks succeed, decrypts the payload back into the original IP packet which it then forwards to the destination inside the internal network.

5 A Flat Zoning Architecture for OT Networks

We now introduce Tableau, a zoning architecture for OT networks that leverages Mondrian in order to achieve flexible, future-proof network management.

Because Mondrian was originally designed for enterprise (i.e., IT) networks, we need to modify its deployment model before it can be used in an OT setting. In Section 5.1, we present this modified deployment model together with the remainder of the Tableau architecture using an example deployment. Then, we discuss additional Tableau features in Sections 5.2 to 5.4.

5.1 A Tableau Production Plant

In a standard Mondrian deployment, all the network zones at each site are connected to the same transition point (TP), which in turn is directly connected to the WAN (Figure 3). Doing so results in a flat zone structure, which is one of Mondrian's key features. In order to preserve this feature when using Mondrian in OT settings, it is necessary to map the inherently hierarchical structure of industrial processes to a flat layout. Further, the use of a single TP per site is not a well-suited approach for OT networks. The reason for this is twofold. First, using a central TP introduces a single point of failure to the data plane. Second, the physical structure of OT networks and the spatial separation between network zones make connecting each zone to the same TP impractical.

In order to flatten the structure of OT networks, we split the network into multiple host zones and a transit network that spans across all traditional network levels, as illustrated in Figure 6. The separation between zones can either

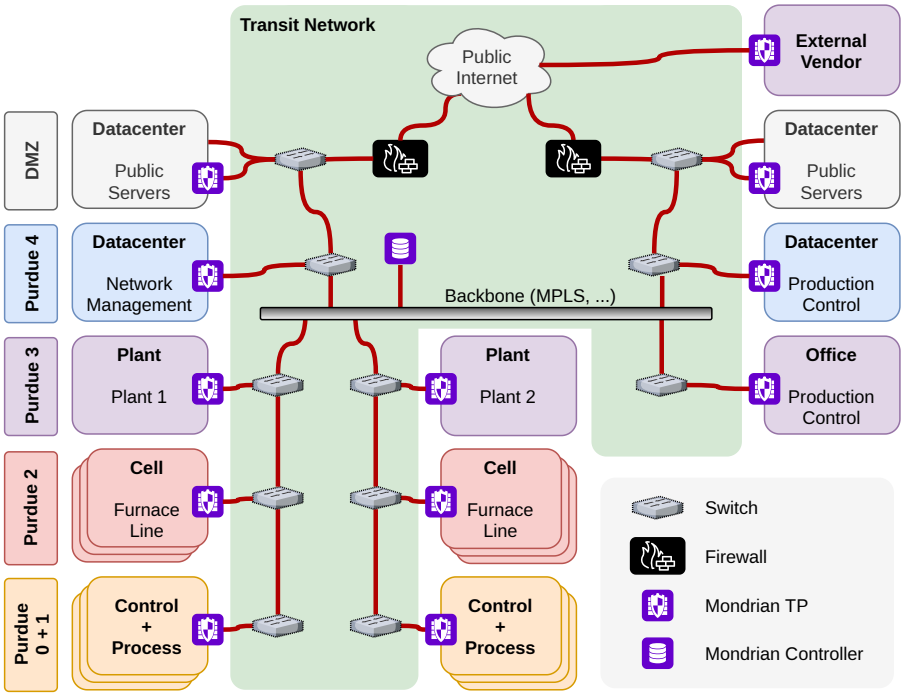


Fig. 6: The TABLEAU equivalent to the Purdue-based network shown in Figure 2.

be physical (i.e., a zone takes the form of a dedicated physical network), or virtual (e.g., a zone consists of one or more VLANs). In either case, the introduction of a transit network ensures that no transit traffic flows through the host zones.

Next, we change the traditional Mondrian deployment model, and instead of connecting each zone to a central TP, we place a TP at the edge of each zone. Only when practical, zones share a TP (not shown in Figure 4). Each TP is then directly connected to the transit network. When traffic leaves a zone, the TP encapsulates it in an encrypted and authenticated tunnel and forwards the traffic over the transit network to the destination zone, where it is decapsulated before being delivered to the final destination.

Many of the zones in Figure 6 can be directly mapped to one of the hierarchical zones in Figure 2 (we indicated the traditional Purdue level of each zone in Figure 6), but there are a number of notable exceptions. We discuss these, together with other notable TABLEAU features, below.

Merging Purdue levels 0 and 1. In today's industrial networks, field devices (i.e., sensors and actuators at Purdue level 0) are usually directly connected to their controllers (Purdue level 1) using a physically separated fieldbus network. Although in the future the functions of the fieldbusses might be taken over by a general-purpose network fabric, the close integration of field devices and controllers will remain critical, both for performance and safety reasons. Therefore,

TABLEAU merges the lowest two Purdue levels and places field devices and controllers in the same zone. This captures both the traditional scenario using dedicated fieldbusses (as depicted in Figure 2), as well as the future scenario where both field devices and controllers are connected to a general purpose (TSN) network fabric.

Integration of IT zones. Because Mondrian was originally designed for enterprise IT networks, it can be used for the management of both IT and OT networks, greatly simplifying the management of converged networks. We demonstrate this in Figure 6 by incorporating an office zone in the network map. Having this flexibility can be especially useful in highly automated or remotely operated plants, where the notion of a traditional control room is fading.

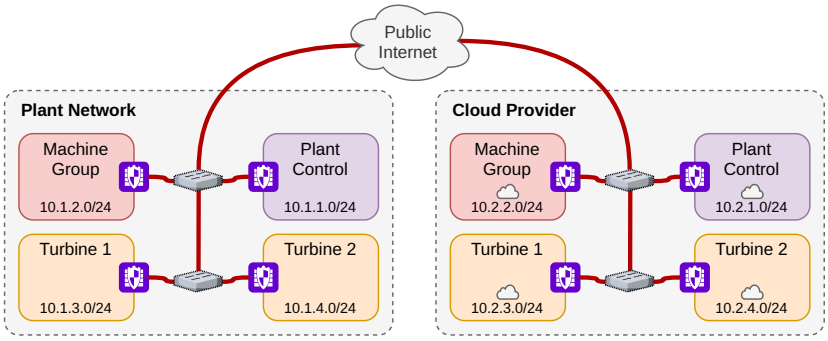
Integration of remote zones. As all data is securely encapsulated during zone transit, the scope of a TABLEAU network does not need to be limited to a single site or domain, and also zone transitions that use the public Internet are possible without the need for additional tunneling mechanisms. In Figure 6 we demonstrate this with the use case of an external vendor that needs to perform device management or security monitoring tasks on a plant's network. In a Purdue network (Figure 2), a dedicated tunnel must be established and maintained between the network of the vendor and the plant operator, and firewalls or jump hosts throughout the Purdue levels must be configured to grant the required access. Evidently, this leads to high management overhead. In contrast, in a TABLEAU network (Figure 6) the external vendor's network can be directly integrated in the networks zone plan. We discuss further benefits of inter-domain zone bridging in Section 5.2.

Open transit network. By only allowing Mondrian encapsulated traffic to flow between network zones, TABLEAU largely eliminates the need for security enforcement within the transit network. We illustrate this in Figure 6 by only placing classical firewalls on the Internet uplinks. An open transit network not only lowers the burden on the network administrators, but also increases the agility of the network.

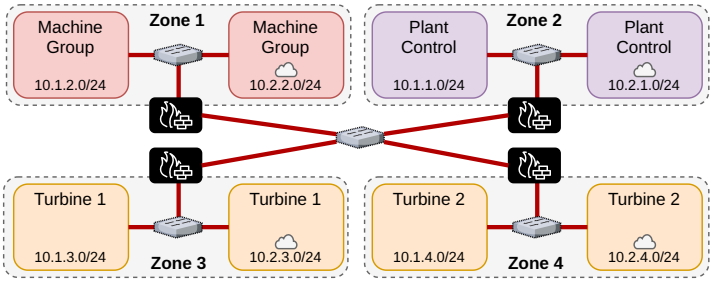
Protection of transit traffic. Because of the hierarchical nature of Purdue networks, zones in a Purdue network need to handle both transit and local traffic. By mixing these two network functions, transit traffic is exposed to tampering by malicious devices in the network zones the traffic traverses. In contrast, TABLEAU splits the network into device zones and a transit network, separating local from transit traffic. Moreover, all inter-zone traffic is authenticated and encrypted while passing over the transit network. Both of these factors reduce the exposure of network traffic to tampering by malicious devices.

5.2 Inter-Domain Zone Bridging

We have already shown how TABLEAU facilitates vendor access to OT networks. Not only can the same approach be used to allow remote workers to connect to



(a) Physical layout



(b) Logical view

Fig. 7: Example TABLEAU topology for a hybrid plant-cloud network.

the company network by running a local Mondrian instance on their laptop, but TABLEAU takes this one step further by splicing network zones across domains.

To make this more concrete, consider the network shown in Figure 7a, the left side of which shows a plant network consisting of four network zones. For economic reasons, the plant operators use multiple cloud services to support the devices in the plant. Concretely, they use a digital twin for each of the turbines, a cloud HMI for remote management of the machine group, and a cloud-based data historian for the plant. These services span across all four network zones in the plant, so in order to maintain zone isolation, the zone structure from the plant is mirrored to the cloud. In today's networks, establishing connectivity from the zones of the plant to those in the cloud would either require bundling traffic from all zones together, or setting up separate tunnels between each pair of zones. Because the former approach breaks the isolation between zones and the later approach induces high management overhead, neither of them is desirable.

In contrast, TABLEAU makes it possible to extend network zones across domains. This means that the physically distant zones pairs (Figure 7a), can be joined to form different subnets of the same logical zone (Figure 7b), without creating additional management overhead. Moreover, because Mondrian uses different cryptographic keys for each zone, zone isolation is maintained across

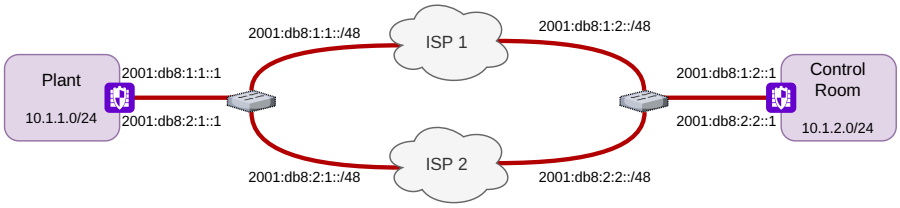


Fig. 8: Example of a TABLEAU deployment on multihomed networks.

the network. Further, this approach is flexible and can be adapted to network operators' needs. For example, instead of extending the same logical zone across multiple domains, the subnets can also be made logically adjacent while remaining in separate zones. This allows for smooth communication to take place between the zones, while still allowing limitations to be placed on which traffic can flow between them.

5.3 Decoupling TP from Logical Zone Connectivity

In a TABLEAU network, the logical connectivity between zones is decoupled from the underlying connectivity of the transition points. Besides simplifying the logical network topology, this also simplifies how redundancy and multihoming can be added to the network. For a concrete example, consider Figure 8, which shows a minimal TABLEAU network consisting of a plant and a remote control room. In order to ensure availability, both the plant and control room are multihomed. To highlight the separation of the logical connectivity between zones and the underlying connectivity on the transit network, we use IPv4 addresses for the former, and IPv6 addresses for the later.

Because the devices inside of the TABLEAU zones are oblivious to the existence of the transit network, multihoming a zone only requires multihoming the zone's TPs. This stands in contrast to traditional multihoming, which directly affects each host in the network [2,16]. It also means that when the connectivity between two zones breaks (e.g., because of link failure), restoring connectivity between the zones (e.g., by falling back a secondary link) only requires intervention on the TPs, and is transparent to the hosts. Although similar properties can be achieved in a Purdue architecture using VPNs, VPNs generate additional administrative overhead, whereas TABLEAU provides these properties by default.

5.4 Backwards Compatibility

In many cases, industrial networks are a brownfield environment. That is, any change to the network must be made while maintaining compatibility with existing devices and structures. To that end, TABLEAU offers two forms of backwards compatibility: partial deployment, and hierarchical overlay.

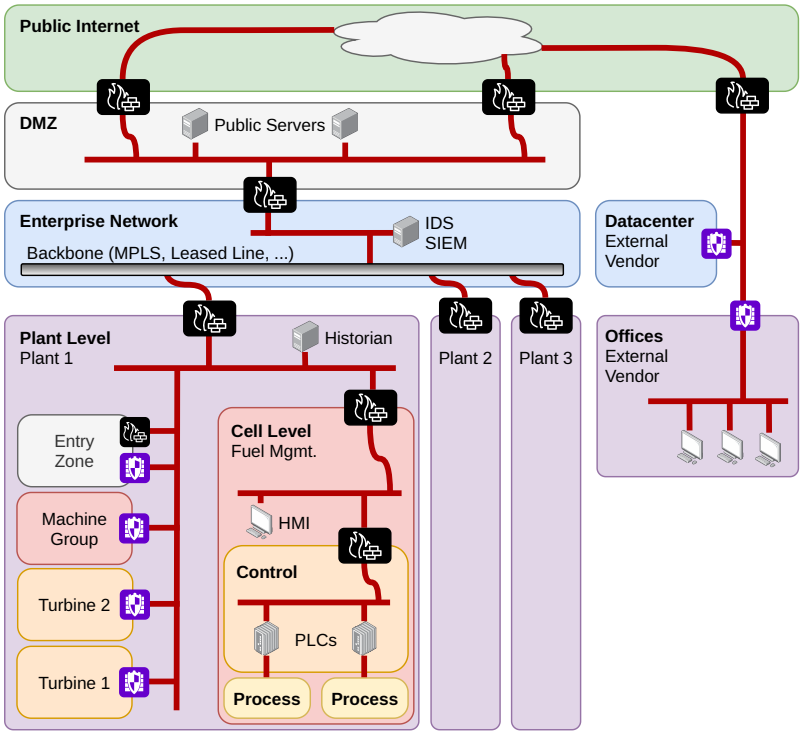


Fig. 9: Example of a partial TABLEAU deployment.

Partial deployment. When it is not possible (or desirable) to convert the full network to a TABLEAU architecture, TABLEAU can be deployed on a subsection of the network instead. For example, when only a single cell in a plant is being updated, it can be desirable to deploy TABLEAU in this cell without changing the other parts of the plant's or organisation's network. We demonstrate this scenario in Figure 9, which shows the same network as Figure 2, but in which one cell is converted to a TABLEAU architecture.

Although only a partial deployment, many of TABLEAU's advantages are retained. Most significantly, there is still full flexibility on how traffic can be routed across the TABLEAU zones. Moreover, assuming that the upstream firewalls are configured to allow TABLEAU traffic to pass through, inter-domain bridging remains possible. We illustrate this in Figure 9 by including the external vendor in the TABLEAU deployment.

In order to facilitate direct communication between the TABLEAU-enabled cell and the plant's network, a dedicated *entry zone* is introduced. This zone acts as a gateway between the Purdue and TABLEAU worlds, giving it a similar function as a demilitarized zone (DMZ) in a Purdue network.

Hierarchical overlay. A TABLEAU network provides full flexibility as to what traffic flows are permitted. This means that it is also possible to implement a

policy that overlays a hierarchical network on top of Tableau. Doing so allows plants operators to convert their network to a Tableau architecture, without having to redraw all security and data-flow concepts at once. Instead, they can initially overlay the same hierarchical policies the network was operating on before, and gradually transition to new network policies and a new security concept from there.

6 Security Aspects

By stepping away from the nested zone model used in today's OT networks, Tableau challenges a widespread design pattern in OT security. Next, we discuss the implications of this architectural change.

Hierarchical network zoning is often motivated by referring to the "defense in depth" security principle: the idea that by layering multiple defense mechanisms behind each other, the security of the system as whole is not compromised when individual defense mechanisms are found faulty. Although it is true that hierarchical network zoning can serve as a form of defense in depth, the true benefits from defense in depth cannot be obtained by using the same defense technique (i.e., firewalls) at multiple points within an organization. Instead, defense in depth requires several independent security mechanisms to be deployed throughout that organization (e.g., firewalls paired with physical security, personnel training, proper patch management, intrusion detection, etc.) [20]. In fact, past studies indicate that having complex, hard-to-maintain firewall structures in a network leads to poor policy management, and thus lowered security [1].

Moreover, as we discuss in Section 3, the threat model for OT networks is changing. Concretely, it is becoming increasingly more likely that attackers will not attack the network level-by-level from the top, but instead will enter the network immediately at one of the lower levels, e.g., after entering the network through a compromised software update [24]. Additionally, the centralized nature of new networking technologies (e.g., TSN and SDN) is reducing the robustness of distributed security enforcement [23]. Both these changes are further reducing the efficiency of hierarchical zoning as a defense in depth measure, and, in the medium to long term, will leave industry with a complex and hard to maintain security system, the security properties of which are based on assumptions that no longer hold.

In contrast, Tableau does not base its security properties on assumptions about the underlying system architecture, but instead simplifies and centralizes security management in order to facilitate the use of modern security tools. Concretely, by consolidating the security policy of a network into a single specification, Tableau facilitates policy simplification, fine-grained zoning, and automated network policy verification. We discuss each of these below.

Policy simplification. Consolidating the network policy into a single specification removes much of the complexity currently encountered in firewall management. This makes policy administration less time-intensive and less error prone. Moreover, the policy becomes easier to audit.

Fine-grained zoning. As discussed in Section 3, an increasing number of devices in the network can function as attacker entry points. In order to limit the impact that a compromised device has on the network, it is desirable to reduce the size of each network zone, thus restricting the lateral movement of an attacker [21]. TABLEAU facilitates fine-grained zoning by lowering the administrative burden required to create and manage additional network zones.

Automated network verification. Not only does TABLEAU make it easier to manually audit network security policies, but aggregating the policy specification at the Mondrian controller also facilitates automated network verification [14]. Automated network verification refers to a set of techniques that make it possible to specify high-level policy goals the network should satisfy, and to automatically verify if a specific network policy satisfies these goals [14]. By doing so, network verification can provide strong guarantees on the correctness of the network policy. Moreover, when performed periodically or at every configuration change, automated network verification makes it possible to dynamically modify the network policy while maintaining a high level of confidence in the correctness of the network policies. This makes it easier and safer to update the network policy as the plant's network evolves.

We anticipate that in most networks, the advantages of trading the hierarchical network model for the flexibility and simplified policy management of a TABLEAU network will well outweigh the disadvantages, resulting in an improved level of security for the network. Nonetheless, in some environments the use of consolidated network policy enforcement may be considered undesirable. We address this issue by introducing *structured heterogeneity*, an approach that adds diversity and redundancy to a TABLEAU network, without interfering with TABLEAU's core features.

The principal idea behind structured heterogeneity is to standardize the interfaces between the various Mondrian components (i.e., transition point, controller, and policy), and to then add diversity to each of them. Concretely, diversity is added to each component as follows:

Transition points: Different TP implementations (e.g., from different vendors) can be deployed in different zones. This limits the consequences of an implementation bug in a specific TP implementation to the zones in which this implementation is used.

Controller: Multiple controller implementations can be deployed in parallel. Each of these controllers connects to the same TPs, and uses the same policy specification. TPs are configured to only permit a zone transition if a threshold number of controllers approve it. This approach also improves network availability, as zone transitions remain possible if one of the controllers is unreachable.

Policy: In order not to increase policy administration overhead, a single policy specification is kept. Instead, we add diversity to the policy *verification*. By verifying the correctness of the policy using multiple methods (e.g., manual

inspection combined with multiple automated network verifiers), this ensures that even if an individual verification tool fails, policy goal violations will be detected.

7 Related Work

Today's standards and models. The architecture and security concepts used in today's OT networks are heavily based on industrial standards and reference models. Although the Purdue Model is often presented as a security model, the original model only discusses information flow [26]. This information model is then used by other standards (i.e., the IEC 62443 [11] series) and architectures (i.e., Cisco and Rockwell Automation's Converged Plantwide Ethernet (CPwE) Architecture). Concrete networks, such as the one in Figure 2 are then based on these derived standards and architectures.

Although Tableau represents a clear break from concrete traditional network architectures such as CPwE, it remains fundamentally compatible with IEC 62443. Concretely, IEC 62443-3-2 [10] does not prescribe a specific zoning model, but states "The organization shall group [control systems] and related assets into zones or conduits as determined by risk." (ZCR 3.1) and "[Control system] assets shall be grouped into zones that are logically or physically separated from business or enterprise system assets." (ZCR 3.2). Tableau provides the tool needed in order to implement these zones and conduits in modern networks. Specifically, zones in a Tableau network map directly to zones as intended by IEC 62443, and conduits are defined by the zone transition policy.

Future-oriented standards and models. The most visible proposal for a future-proof OT architecture is the NAMUR Open Architecture (NOA) [19]. NOA places a secondary *monitoring and optimization* network in parallel to the existing *core* automation infrastructure. Data is fed from the core network into the secondary network through data diodes, where it can be analyzed. Control commands from the secondary network are transferred back to the core network through a request verification gateway. Although NOA has the advantage that it leaves the existing automation network largely untouched, the functionality of the secondary network stays limited to a supporting role. This means that NOA does not address how to handle changes to the core of the automation architecture, e.g., the introduction of virtual automation functions or the increasing prevalence of highly-autonomous remotely controlled facilities.

Another prominent standardization effort is the Reference Architectural Model for Industrie 4.0 (RAMI 4.0) [5], which was developed to support Industry 4.0 initiatives. However, RAMI 4.0 focuses on the representation and management of assets, and does not discuss network topologies.

8 Conclusion

The rise of the IIoT and the ongoing IT/OT convergence are challenging the ways in which we defend OT networks. If we ignore this reality, the security

properties of our networks will slowly erode while administrative overhead will grow. Instead, we must reevaluate the security concepts used in the OT world, and adapt them to reflect the current—and future—state of the network.

In this paper, we introduced the Mondrian-based TABLEAU zoning architecture. TABLEAU provides the flexibility required by contemporary industrial workloads, lowers administrative overhead, is brownfield-compatible, and facilitates the use of modern security practices. Moreover, because Mondrian has its roots in IT networks, TABLEAU draws from the many years of experience the IT world has with managing the technologies that the IIoT and IT/OT convergence are introducing to our industrial networks.

References

1. Al-Shaer, E.S., Hamed, H.H.: Modeling and management of firewall policies. IEEE Transactions on Network and Service Management **1**(1), 2–10 (apr 2004). https://doi.org/10.1109/tnsm.2004.4623689
2. Bates, T.J., Rekhter, Y.: Scalable Support for Multi-homed Multi-provider Connectivity. RFC 2260 (Jan 1998). https://doi.org/10.17487/RFC2260, https://rfc-editor.org/rfc/rfc2260.txt
3. CISCO: IT/OT convergence. https://www.cisco.com/c/dam/en_us/solutions/industries/manufacturing/ITOT-convergence-whitepaper.pdf (2018)
4. Cisco Systems and Rockwell Automation: Ethernet-to-the-factory 1.2 design and implementation guide. https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/EttF/EttFDIG.pdf (jul 2008)
5. Deutsches Institut für Normung: DIN SPEC 91345:2016-04: Reference Architecture Model Industrie 4.0 (RAMI4.0) (2016), Technical Standard
6. Greenfield, D.: Is the Purdue Model still relevant? Automation World, https://www.automationworld.com/factory/iiot/article/21132891/is-the-purdue-model-still-relevant (2020)
7. Hegrat, B., Langill, J., Peterson, D.: S4x19 panel discussion: Is the Purdue Model dead? https://s4xevents.com/past-events-2/s4x19/ (2019)
8. IEEE 802.1: Time-sensitive networking (TSN) task group. https://1.ieee802.org/tsn/ (2020)
9. IEEE 802.1, IEC SC65C/WG18: IEC/IEEE 60802 TSN profile for industrial automation (draft d1.2). https://1.ieee802.org/tsn/iec-ieee-60802/ (2020)
10. International Electrotechnical Commission: IEC 62443 standard series: Industrial communication networks - IT security for networks and systems, Technical Standard
11. International Electrotechnical Commission: IEC 62443-3-2:2020 security for industrial automation and control systems - part 3-2: Security risk assessment for system design (2020), Technical Standard
12. Koelemij, S.: The Purdue Reference Model outdated or up-to-date? https://otcybersecurity.blog/2020/06/08/the-purdue-reference-model-outdated-or-up-to-date/ (2020)
13. Kwon, J., Hähni, C., Bamert, P., Perrig, A.: Mondrian: Comprehensive inter-domain network zoning architecture. In: Proceedings of the Symposium on Network and Distributed System Security (NDSS) (2021). https://doi.org/10.14722/ndss.2021.24378

14. Li, Y., Yin, X., Wang, Z., Yao, J., Shi, X., Wu, J., Zhang, H., Wang, Q.: A survey on network verification and testing with formal methods: Approaches and challenges. IEEE Communications Surveys & Tutorials **21**(1), 940–969 (2019). https://doi.org/10.1109/comst.2018.2868050
15. Lo Bello, L., Steiner, W.: A perspective on IEEE time-sensitive networking for industrial communication and automation systems. Proceedings of the IEEE **107**(6) (2019). https://doi.org/10.1109/jproc.2019.2905334
16. Matsumoto, A., Fujisaki, T., Hiromi, R., Kanayama, K.: Problem Statement for Default Address Selection in Multi-Prefix Environments: Operational Issues of RFC 3484 Default Rules. RFC 5220 (Jul 2008). https://doi.org/10.17487/RFC5220, https://rfc-editor.org/rfc/rfc5220.txt
17. Miklovic, D.: IIoT will change our view of CIM; the Purdue Model is becoming dated. Industrial Transformation Blog, https://blog.lnsresearch.com/iiot-will-change-our-view-of-cim-the-purdue-model-is-becoming-dated (2015)
18. Mission Secure: Is the Purdue Model relevant in a world of industrial Internet of Things (IIoT) and cloud services? https://www.missionsecure.com/blog/purdue-model-relevance-in-industrial-internet-of-things-iiot-cloud (2021)
19. NAMUR: NAMUR Recommendation NE 175: NAMUR Open Architecture – NOA Concept (2020), Technical Standard
20. NSA: Defense in depth: A practical strategy for achieving information assurance in today's highly networked environments (2012)
21. Paloalto Networks: 2020 unit 42 iot threat report. https://unit42.paloaltonetworks.com/iot-threat-report-2020/ (2020)
22. Sauter, T., Soucek, S., Kastner, W., Dietrich, D.: The evolution of factory and building automation. IEEE Industrial Electronics Magazine **5**(3) (2011). https://doi.org/10.1109/mie.2011.942175
23. Scott-Hayward, S., Natarajan, S., Sezer, S.: A survey of security in software defined networks. IEEE Communications Surveys & Tutorials **18**(1), 623–654 (2016). https://doi.org/10.1109/comst.2015.2453114
24. Temple-Raston, D.: A 'worst nightmare' cyberattack: The untold story of the solarwinds hack. https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack?t=1619951063586 (2021)
25. VDI/VDE Gesellschaft Mess- und Automatisierugnstechnik: Cypber-physical systems: Chancen und nutzen aus sicht der automation. Tech. rep. (2013)
26. Williams, T.J. (ed.): A Reference Model for Computer Integrated Manufacturing (CIM). Instrument Society of America (1989)
27. 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 Industrial Electronics Magazine **11**(1) (2017). https://doi.org/10.1109/mie.2017.2649104