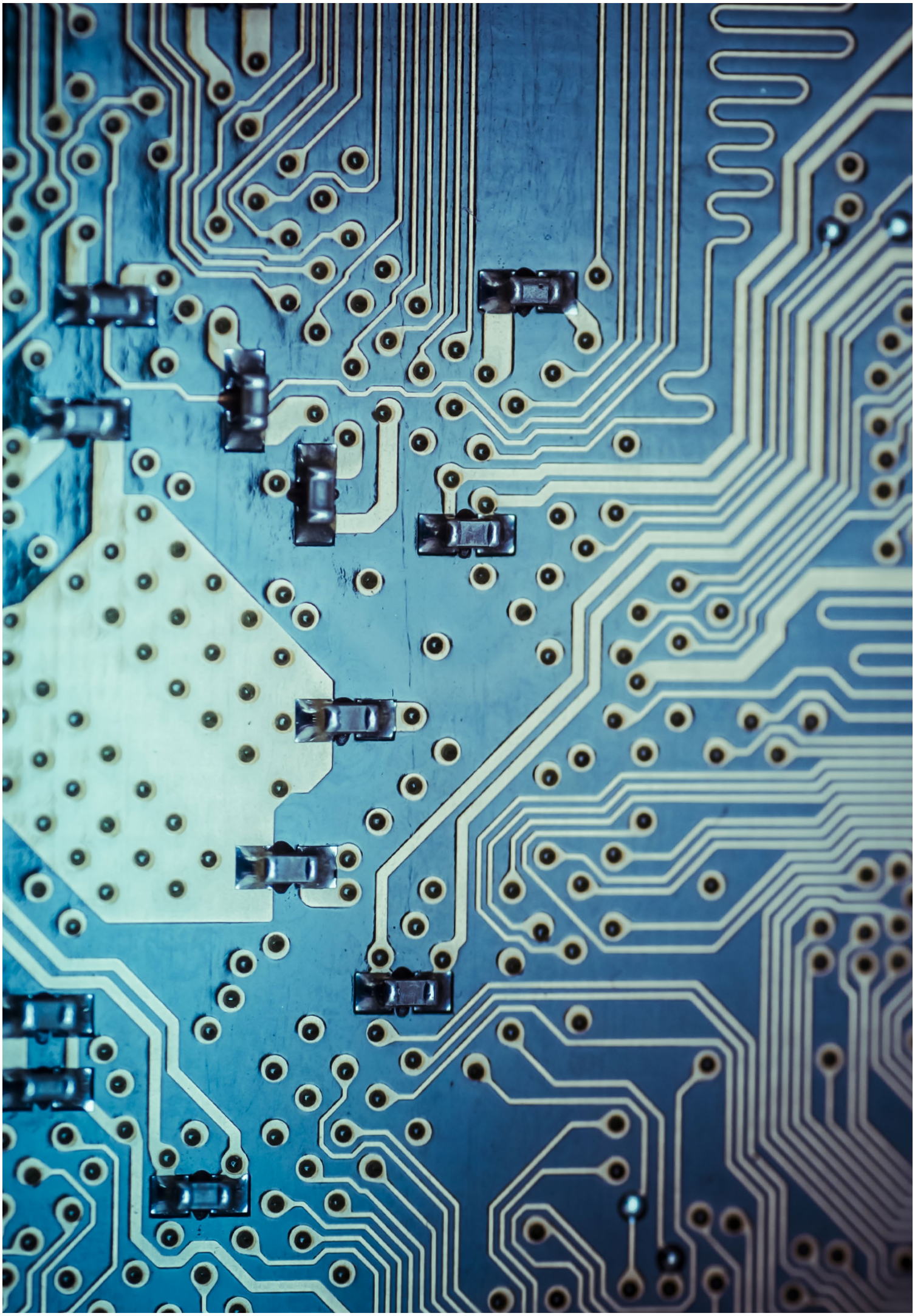
Deloitte.

Beyond Remote Access

Intelligent IT/OT connectivity to supported machines and applications

MAKING AN IMPACT THAT MATTERS since 1845



Introduction

The need for secure, robust remote access to equipment, machines, and systems is obvious. With the advent of IoT and Industry 4.0, information, interaction with equipment on the shop floor and communication with devices can be accomplished in ways we could scarcely imagine a decade ago. Manufacturers requiring remote access to industrial equipment and machines owned and used by third parties are becoming more common. Where previously support or maintenance personnel was dispatched to the equipment location, remote access is now the norm.

Implementation of secure remote access is not a silver bullet though. Connectivity into customer networks and environments cannot be taken for granted as customer networks and access points move toward more secure profiles given the major security risks faced every day. We must provide connectivity options that are robust and reliable, and leave no doubt that they themselves do not present a security risk to our customers.

Cybersecurity threats, including ransomware, data theft, and even internal espionage, continue to gain momentum within the OT domain on the factory floor. They call for a vigorous, fail-proof mechanism for remote access granted only to authorized personnel and without trusting any single stakeholder: user, network, equipment or communication method.

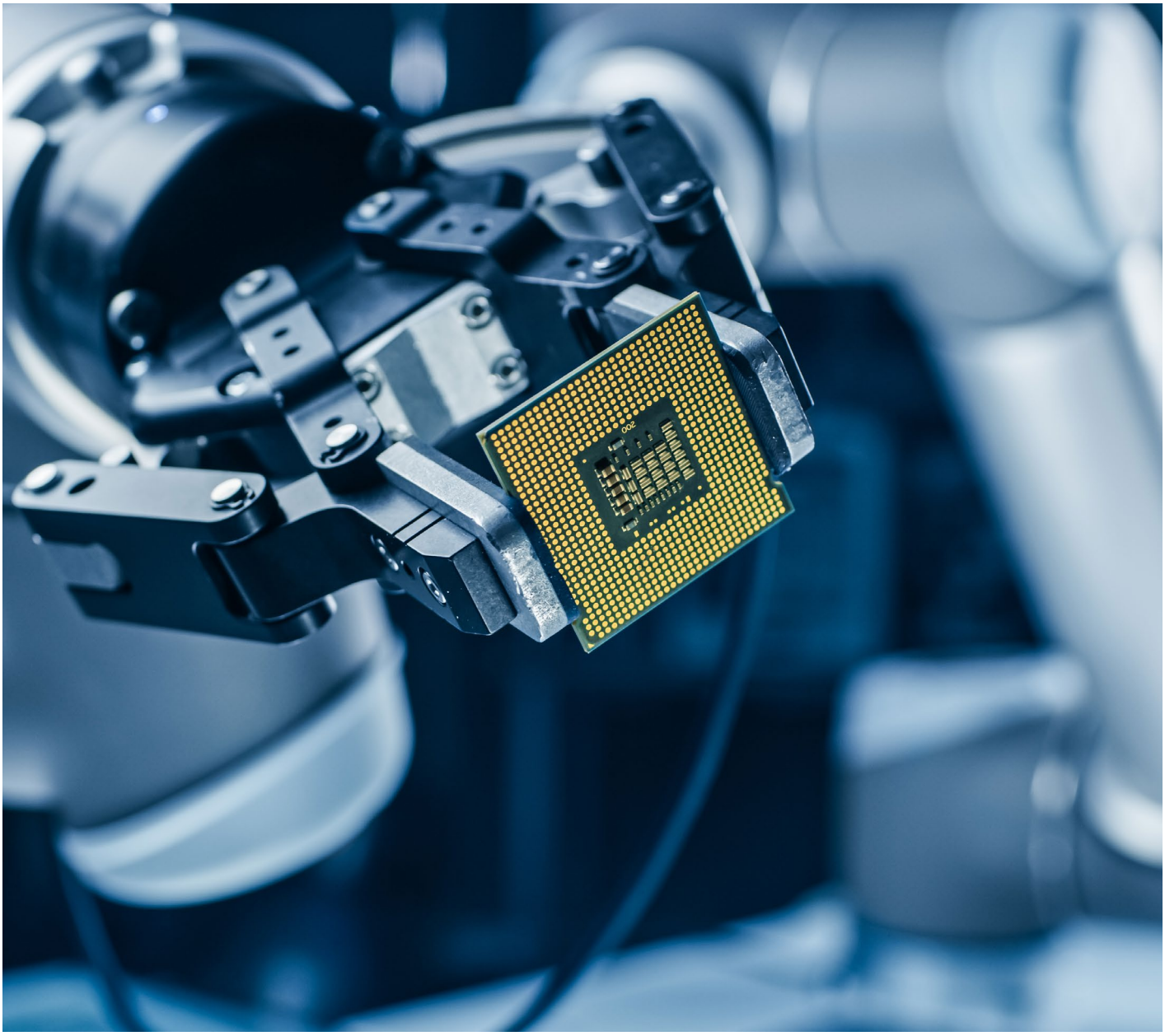
The benefits of a successful implementation are of course real. In industrial environments, remote access to supported machines and applications forms a critical pillar of issue resolution, configuration management and deployment of remote updates, and can be leveraged by multiple stakeholders at different points in a product's lifecycle. With the proliferation of software components, high ROI expectations on digital services and the drive for more efficiency and sustainability, especially in aftersales, remote access furthermore becomes one of THE key enablers to future-proof your business. Adapting to customer ecosystems and their prerequisites for remote access, on the other hand, is not a valid option due to exponential costs and complexity. A north star metric for remote access should start with the following:

To provide a high-level standardized, secure and scalable implementation plan and reduce the complexity of achieving remote access

This paper is based on real-world considerations and will outline some opportunities and challenges in achieving remote-access equipment support within your organization.

Industrial Remote Access

Over the past few decades, with implementations of Industry 4.0 transformations powered by the Internet of Things, we have come across few challenges that come in the way of successful practical rollout and enterprise level adoption.



Complex Support Ecosystem

Current remote-access requirements and processes are complex and heterogeneous across different product lines and clients. Tools and user access are not standardized, with independent support mechanisms across product lines. Each may have different requirements for remote access. Some equipment may need direct access to control systems (PLC), while others require desktop access for debugging and diagnostics. A standardized system landscape is mission-critical for proactive support and maintenance.

Dependency on the Customer Environment

Vendor remote access is heavily dependent on the customer environment for network, hardware, and user access (password reset, firewall rules, etc.). There are often limitations on security, such as user account management and networking (ports access). IT security restrictions for firewalls and ports have increased, leading to greater complexity. Any external service provider entering the ecosystem with its own hardware gateways, protocols, software constitutes a significant security risk.

External suppliers with different remote-access approaches

Different suppliers adopt custom-built rebranded solutions for remote access – which only drives complexity for support teams. The existence of multiple points for remote access is not only cumbersome from a setup perspective, it creates an increased attack surface for cyber threats.

Adopting a platform approach to remote access

All stakeholders must be aligned on the process, tools, and methods for unified remote access and the possibility of a platform-based approach with clear ownership. A future-ready cloud platform with support for multiple hyperscalers can enable future business models and uses. The solution must also be thought through from an OT-based perspective, as opposed to traditional IT-based remote access.

A solution conformant to ISA-95 standards will help boost efforts towards standardization.

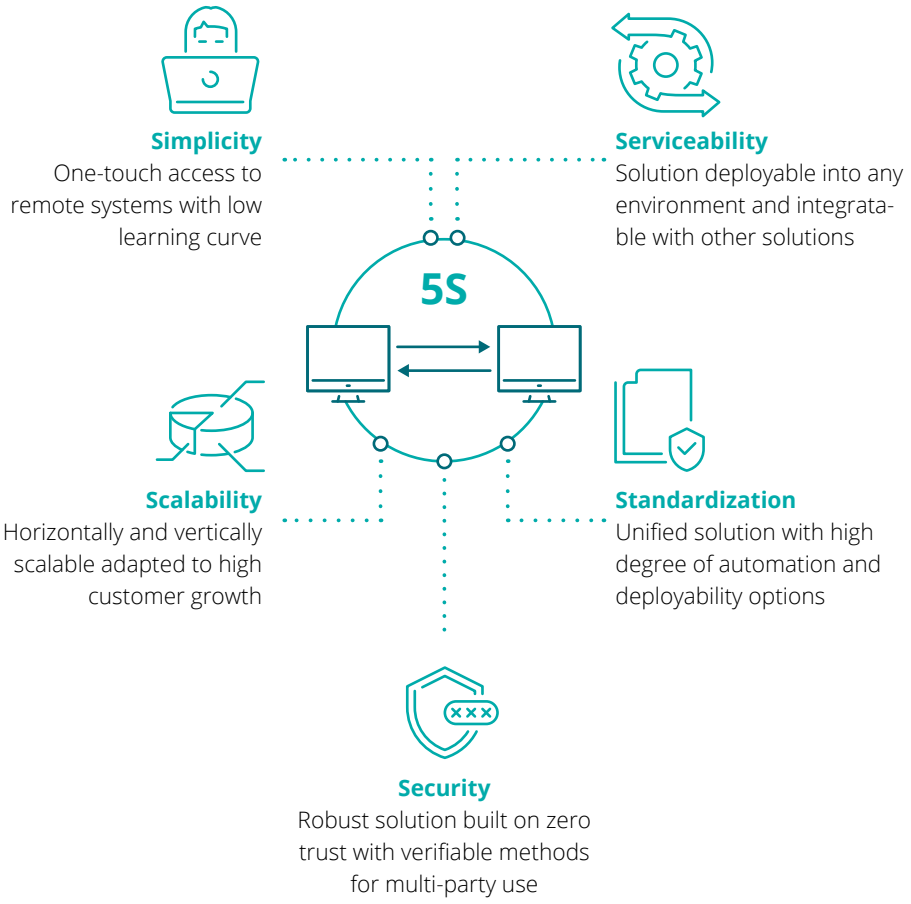
Centralized solution based on 5S principle

Consider the 5S principles of Simplicity, Scalability, Security, Standardization, and Serviceability shown in Figure 1. This solution is based on zero-trust network access and provides much-needed confidence against cyber risk. Built-in audit logging, observability (MELT), and intrusion detection with endpoint security increase customer trust in the solution. Suppliers are also streamlined into the remote access process to provide them with unified access.

Tight coupling with support efforts

Methods for tightly integrating remote access into the support framework and which evolve from reactive to proactive to preventative support must be thought through during the architecture phase. User-centric design with minimal access complexities coupled with zero-touch commissioning of hardware and software during first-time installation will greatly improve user satisfaction.

Fig. 1 – 5S principles for remote access system design



State-of-the-art Vendor Remote Access

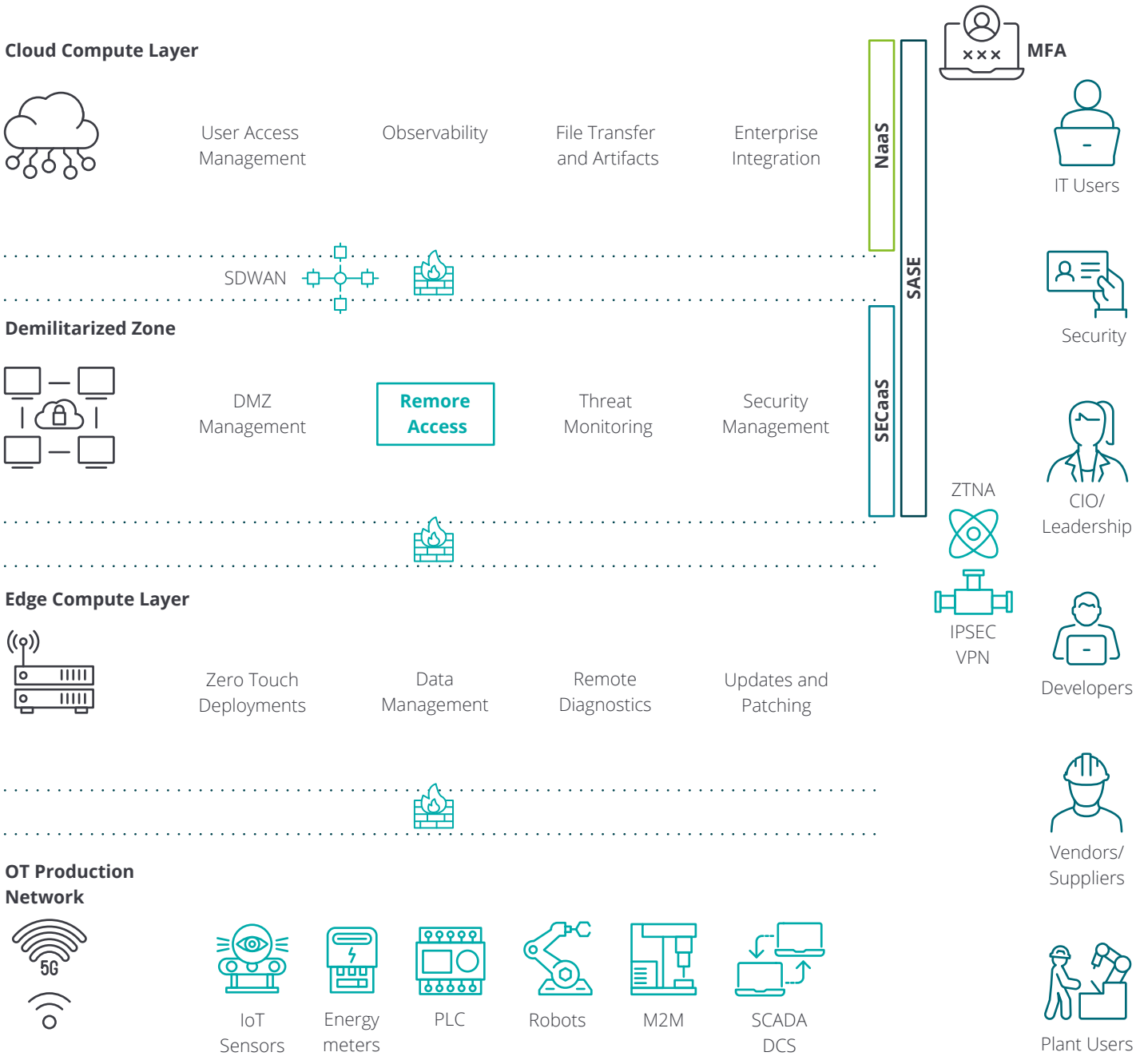
In our specific context, we are focusing on vendor remote access and on the ability to manage equipment and applications in the field. This can be machines and equipment in remote locations or, more often, within customer environments. To better understand the challenges we will review a standard architecture approach. Secure Access Service Edge (SASE, pronounced 'sassy') is a cyber-security concept defined by Gartner as The Future of Network Security in the Cloud. SASE describes several technologies across the security and networking environment for deployment as a set of services.

SASE is a framework rather than a specific technology. Multiple vendors are stepping up to help vendors and customers adopt the model. Well-defined SASE architecture identifies users and devices and applies policy-based security for secure access. These policies can be managed by both vendor and customer to ensure security at all levels of access. SASE focuses on two specific layers. Security-as-a-service (SECaaS) allows the designated service provider to integrate security services into an enterprise infrastructure. This requires the customer to allow a trusted security provider remote access to systems.

The second layer is Network-as-a-Service (NaaS). It provides state-of-the-art network management and security using forwarding rules, VPN, and SD-WAN technologies. This framework for network architectures combines Wide Area Networking (WAN) and cloud security, leveraging several cloud-native security approaches such as Secure Web Gateways (SWG) and Zero Trust Network Access (ZTNA).

Figure 2 illustrates this model in the context of the OT environment. Access to remote systems is required and must be controlled by both the customer network and the vendor providing the services. This combination of technologies provides for joint security ownership between customer and vendor and allows for secure access to systems and applications with minimal risk. Access to customer systems is managed from a central cloud-based platform across all users, including support personnel and customer systems requiring access.

Fig. 2 – Remote Access Reference Architecture based on SASE



The Impact of Industrial 5G

Ubiquitous connectivity is one of the major drivers of Industry 4.0, and organizations are struggling to adopt an IoT connectivity strategy that is readily available, secure, and robust enough to support the expected flood of data. The widespread adoption of Industrial 5G networks can massively improve reliability, speed, security, and performance. By design, 5G is capable of hosting multiple logical networks inside a physical network providing flexibility for different use cases.

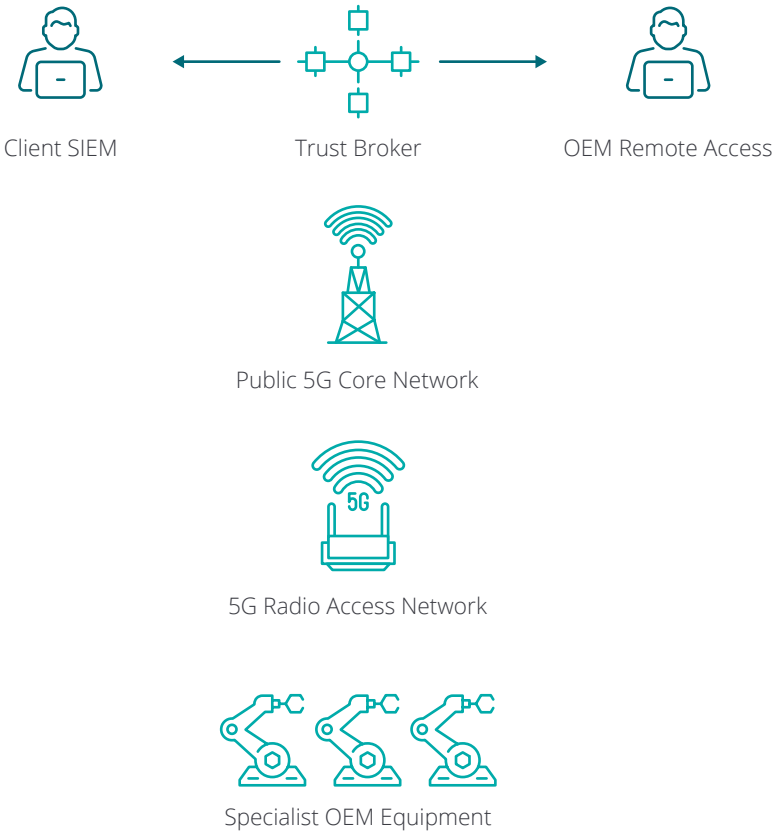
A tailored 5G network can be configured as an NPN (non-public network) for local data aggregation within an OT environment. Through dedicated radio equipment with plug-and-play deployment capability, data acquisition and control can be enabled at ultra-high speed. This network then interfaces with the public network through the next-gen firewall in OT to provide to-and-from traffic exchange. Industrial 5G networks can thus play a crucial role in client deployable brownfield scenarios to connect to OEM assets independent of existing legacy OT/IT networks.

An additional benefit of 5G networks is they can be overlaid on existing environments with minimal cabling. Current ranges and bandwidth do not require expensive cabling to provide support for an isolated network. As mentioned, this overlay network of devices can be built with state-of-the-art technology, smart firewalls, and restricted access to the corporate network. These are all additional security features for vendors who require access to minimize maintenance and support efforts on equipment and applications. Private 5G network infrastructure thus creates a safe, super scalable and easy-to-implement mechanism to allow third-party and system integrators access to essential device data.

This completely removes dependencies on customer network infrastructure, policies, processes, and personnel , thereby shortening time to fix - MTTR (mean time to repair), thereby creating value for the end customer.

Figure 3 shows an interesting use case in which the OEM intends to manage and maintain assets at a restrictive client install location. When equipment is leased in an AaaS model, management and maintenance fall under the purview of the OEM. In such a scenario, a private 5G network with radio access point can be easily deployed at short notice and in isolation to the existing network infrastructure. Data communication is handled at the trust broker layer where both the OEMs and Client SIEM team have access to data based on API calls. This creates transparency and trust in the system.

Fig. 3 – 5G Private networks for retrofit service implementation



Security and Zero Trust

The foundational tenets of information security are the triad of Confidentiality, Integrity, and Availability, in order of priority. But when it comes to the OT or the production network, the order changes. Availability, integrity, and latency take center stage with their direct impact on uptime, reliability, safety, and business continuity. Confidentiality is important, but takes a backseat in industrial applications. OT is where cyber security incidents become real-world safety incidents, so it must be well designed. Preventing physical harm to factory workers, machinery, the environment, and end users is fundamental. In a brownfield context with traditional and legacy systems, incorporating security by design becomes almost impossible without a major overhaul of technology and equipment. A systematic and robust program to reinforce security through a coherent set of practices must be targeted to build systems resilient to sophisticated cyberattacks.

Zero Trust Architecture

Zero trust is one such methodology for implementing security. It is defined as a paradigm of security that assumes that all actors, applications, resources, and networks, regardless of location, priority, source, or destination, are non-trustable until proven otherwise. Every attempt to connect to the network must be identified, authorized, and authenticated by a trusted source. Zero trust divides the network into data plane and control plane. Control plane is where the trusted engine resides, with policies built in for granting access to users and applications via the network. The resources (system, data, application) reside in the data plane, where the exchange happens.

How is zero trust achieved?

Implemented as a series of measures, it includes multi-factor authentication, device posture assessment, network micro-segmentation, and real-time monitoring. MFA requires users to provide additional forms of authentication such as password, secure token, biometric-based hardware key, etc. to declare trust and prove credibility for access. Device posture takes into consideration system parameters like up-to-date operating system, security patches, up-to-date antivirus, etc. for access. Segmenting assets into multiple small VLANs reduces the attack surface. Potential attacks are limited to the specific segment rather than the entire network. Real-time network traffic monitoring sniffs for any suspicious signs of attack, and response measures are in place for mitigation.

Secure implementation for OT

So how does this translate to remote access to the OT domain? Retrofitted appliance-based network devices are available as network watchdogs in the OT network. OT resources like PLCs, SCADA systems and their control servers in a typical production area are micro segmented into isolated VLANs, with access for applications and users limited to approved resources. Instead of exposing network parameters like IP addresses and ports, the remote access engine abstracts them into a HTML5-based web session that plays on the remote connected device, minimizing knowledge leakage on network setup to potential adversaries. What's more, security increases by providing access on a per session basis with dynamic policy control. Operations like file transfer, remote diagnostics, log data analysis, remote patching, and firmware updates are all centrally monitored and orchestrated to guarantee worry-free remote access across the enterprise.

Applications and Business Case

All this effort must provide value to prospective stakeholders. Below we describe some applications for remote access and outline the case for moving forward.

Remote troubleshooting with specialists

Failure of critical machinery or equipment can shut down entire production. Rapid troubleshooting and corrective responses are called for. Vendors, OEM specialists, and system integrators with a secure channel for accessing OT systems can make a significant impact. Secure remote access not only cuts costs, it significantly reduces unplanned downtime. Remote access, coupled with continuous system monitoring and assisted augmented reality applications, are creatively altering maintenance ecosystems forever.

Central management with reduced resources

For enterprises with multiple production and deployment facilities across the globe, it makes sense to have a central management team to monitor and provide maintenance services rather than having redundant teams at each facility. Cost efficiencies are gained, while removing remote staffing and training resources. Standardized solutions create tighter landscapes across users and reduce inefficiencies.

Orchestrating remote system updates

While over-the-air system updates are common and standard for IT systems and mobile systems, all OT systems by design and age are not compatible. Security patches, device updates, and firmware refreshes must be orchestrated and manually monitored for success. The ability to perform system updates from halfway across the globe during a shift downtime is a blessing, minimizing transportation (6 Sigma and 8 types of waste) and improving productivity.

Federated control for building trust with zero trust

Built-in continuous observability with secure remote access provides stakeholders with much-needed visibility: clients, customers, vendors, partners, system integrators, component OEMs, service providers, etc. The zero-trust paradigm focuses on resource protection in that trust is never granted implicitly but rather constantly evaluated, in essence creating much-needed trust in the system.

The examples above not only prove the business value of remote access but drive home the positive impacts of the global ESG Index. Environmental sustainability and governance are now crucial, and less travel and reduced carbon footprint are key benefits of enterprise-scale remote access.

Next Steps in your Journey

Secure controlling, management, and monitoring of access to external vendors, partners and internal users is key to a successful remote access program. We recommend the following steps to establish this key enabler for your (cyberphysical) products:

1. Define a common strategy between functions (most likely Sales, Aftersales & Service, R&D and IT) to create the right setup and alignment for remote access and your Go2Market. Can your standardized remote access concept be part of the contract and prerequisite for negotiated SLAs?
2. Align with your suppliers on a standardized concept, especially in case of low vertical integration
3. Define responsibilities in your organization. Who is responsible for remote access? IT? After sales & Service? R&D?

We are happy to support you with client insights and best practices.

Glossary

01. Application Programming Interface (API): A set of rules and specifications that software programs follow to communicate with one another; serves as an interface between different software programs
02. Cloud Access Security Broker (CASB): An on-premise or cloud-based software that sits between cloud service users and cloud applications and monitors all activity while enforcing security policies.
03. Domain Name System (DNS): The hierarchical and decentralized naming system used to identify computers reachable through the Internet or other Internet Protocol networks.
04. Demilitarized Zone (DMZ): A physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted, usually larger, network such as the Internet.
05. File Transfer Protocol (FTP): A standard network protocol used to transfer computer files between a client and a server on a network.
06. Hyper Text Transfer Protocol Secure (HTTPS): Protocol for secure communication via a web browser on the Internet that uses the Secure Sockets Layer (SSL) protocol for encryption.
07. HTML5: A markup language used for structuring and presenting content on the World Wide Web.
08. Intrusion Detection System (IDS): A hardware device or software application that monitors a network or system for malicious activity.
09. Internet Protocol security (IPsec): Network protocols that authenticate and encrypt data packets
10. Identity and access management (IAM): A framework of policies and technologies to ensure that the right users have appropriate access to technology resources.
11. ISA-95 – A standard from the International Society of Automation for developing an automated interface between enterprise and control systems
12. Local Area Network (LAN): A computer network that connects computers and devices (including machines) in a building, factory, office, or other relatively small area.
13. MELT: Observability mechanisms comprised of Metrics, events, logs and traces.
14. Multi-factor authentication (MFA): A type of access control that grants access only after providing at least two forms of authentication.
15. Mean Time to Repair (MTTR): The average time it takes to repair and recover from a product or system failure.
16. Original Equipment Manufacturer (OEM): A company that produces parts and equipment that can be marketed by another manufacturer.
17. Operational Technology (OT): The practice of using hardware and software to control industrial equipment, primarily interacting with the physical world.
18. Programmable Logic Controller (PLC): A robust industrial computer used for automated control of manufacturing processes.
19. Role-Based Access Control (RBAC): A method of controlling access to the resources of a computer or network based on defined roles assigned to individual users within an organization.
20. Remote Desktop Protocol (RDP): A proprietary protocol which provides users with a graphical interface to connect to another computer over a network connection.
21. SASE: Technology used to deliver wide area network and security controls as a service directly to the source of connection rather than to a data center
22. Site to Site VPN Tunnel: Encrypts traffic at one end and sends it to another site over the public Internet where it is decrypted and routed on to its destination.
23. Service Level Agreement (SLA): A formal commitment between a service provider and a customer that addresses specific aspects of the service provided such as quality, performance, and responsibilities.
24. Security Information and Event Management (SIEM): Supports threat detection, compliance and security-incident management through the collection and analysis (both near real-time and historical) of security events.
25. Security Assertion Markup Language (SAML): An open standard for exchanging authentication and authorization data between parties and an identity provider and service provider.
26. Software-defined Wide Area Network (SD-WAN): A wide area network that uses software-defined network technology, such as communicating over the Internet using overlay tunnels which are encrypted.
27. Zero trust network access (ZTNA): A set of technologies and functionalities that enable secure access to internal applications for remote users by limiting implicit trust.

Authors and contacts

Kai-Uwe Hess
Partner
Lead Technology Strategy & Architecture
kahess@deloitte.de

Marcel Mehdianpour
Director
Lead Technology Strategy & Architecture
mmehdianpour@deloitte.de

Joey (Anthony) Bernal
Senior Specialist Lead
Technology Strategy & Architecture
anbernal@deloitte.de

Bharath Sridhar
Specialist Lead
Technology Strategy & Architecture
bhsridhar@deloitte.de

Deloitte.

Issue 05/2023