The New Remote Access

Take action to be ready and compliant

Introduction

In the pervasive reality of the Industrial Internet of Things (IIoT), or Industry 4.0, the ability to access industrial machinery, or "Remote Access," enables technicians to remotely monitor machine performance by using data relayed via computer networks. This works both within the confines of the industrial plant, or via routers and security protocols across wide area networks, in principle allowing operators to do their job from anywhere in the world. A full Industry 4.0 solution will typically go further and use this connection to automatically collect machine data and use this footprint to drive a whole range of applications and data analysis that will allow the user to monitor machine performance and performance trends, improve quality, optimize machine downtime, and predict required maintenance actions. But even the most basic incarnation of the Industrial Internet of Things, **the ability for operators and service technicians to access the machine remotely, is as simple as it is compelling for its promise of immediate return-on-investment:**

In case of a problem, a service technician (maybe even a specialist working for the machine manufacturer) can securely and remotely access all pertinent machine data to assess the issue, initiate remedial work, or assist the on-site operator with trouble-shooting. One of our OEM clients, a machine builder with 5000 connected machines around the world, has reported that 80% of all service requests can be resolved completely on-line without requiring any on-site visit. This, in turn, saves this particular machine builder over $2M per year in travel costs - this is but one success story from the ei^3 library. The machine owner, on the other hand, benefits from having problems resolved quickly, thus reducing costly machine downtime.

The Covid-19 pandemic that spread across the world in January of 2020 has required the adoption of social distancing rules in many countries, and as a result has disrupted industrial production to an extent never before seen in history. The ability to remotely manage industrial production is gathering new momentum. This time, however, **the focus is not on remote service to manage exceptions (such as mechanical problems or faults), but on using remote operators as a routine means to manage operations.**

This has significant implications for the remote access technology itself and requires a careful re-assessment of the requirements concerning security, corporate policies, deployment scenarios, and usage monitoring.

Remote Access

A very simplistic, but deficient, remote access implementation may be achieved by ensuring that two layers of connectivity operate.

First, the networking layer that provides data level access from the remote operator's work station to the industrial machinery. In order for data packets to flow, usually a gateway is deployed that relays these packets from some wide area network to the machine controller inside the industrial machine. In reality, additional configuration is needed to allow network-level access to the gateway via the Internet, which often requires sophisticated security protocols to be in place. For example, implementors might resort to packet forwarding, open ports, and "holes" in corporate fire walls. Simple username/passwords would limit access to those gateways to authorized persons.

Second, a method to remotely control the machine controller must be in place. Some types of machine controllers ("PLCs") have their own management software that can be used. Often times "remote screen" sharing tools are used to access the PLCs' HMI interface, essentially allowing the remote operator to access the screen display of the machine in the same way that the on-site operator would interact with the physical screen/ keypads on the machine itself. The remote operator would thus gain full and uninhibited access to the same capabilities that are also available to the on-site operator.

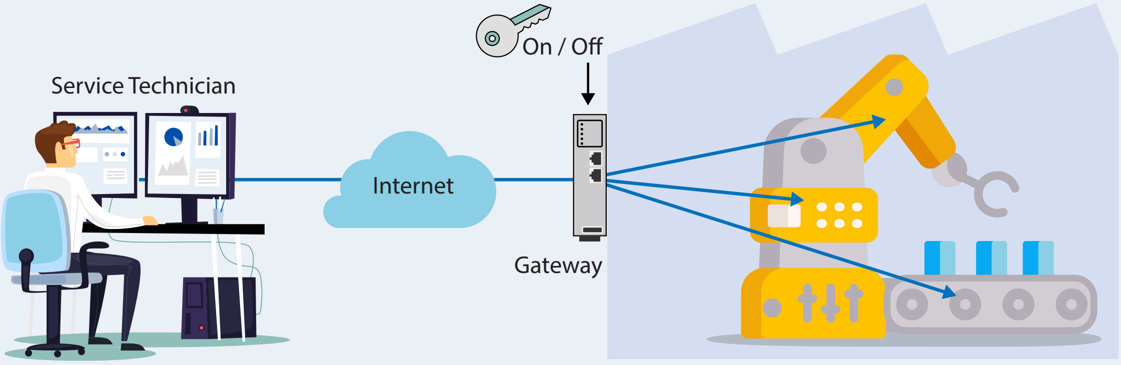


Figure 1

A basic remote access system may consist of a gateway that allows service technicians direct access to industrial equipment. In practice, operational security is often achieved through a manual key switch that enables or disables access.

The short description above may not give full justice to the more sophisticated implementations that are currently in operation. However, it serves to highlight the range of issues, which are potentially posed by simplistic remote access solutions:

- allowing uncontrolled external IP access to the shop floor is a disaster waiting to happen, no matter how sophisticated the authentication protocols that are employed. What is at stake here is the loss of information and data, loss of production when machinery goes offline for unknown reasons, and even physical damage to costly machinery and industrial assets. In short, inbound connections through firewalls are the nightmare of every corporate IT department.

- usernames and passwords do not provide adequate protection when external parties are accessing critical information. Consider the case when the external party is a service technician from your machine supplier, of which, presumably, there is more than one. Would every service technician receive their own unique username/password for every machine with every operator? More likely a single username/password pair would be used for groups of machines or service technicians, leading to an inability to withdraw access rights to such usernames. As a result, these passwords become common (group-)knowledge and therefore provide no security at all.

- once provided with access to the gateway box, there is little in the way of preventing access to all assets on the shop floor network. The service technician will most likely be able to access any asset and exercise any function as they see fit.

The list of security concerns goes on. But despite these obvious limitations, simple secure remote access solutions are being deployed, and in many cases that is OK - because the solution is intended to be used in exceptional circumstances only, for example, when an issue has lead to downtime that is being resolved by the service technician now. In such deployments often a physical “key switch” is used to provide power to the gateway and, thus, enable its operation. Once the issue is resolved, the key switch would be turned off to disable the gateway by cutting main power. Thus, these solutions achieve their goal as a tool for **exception management** but better and more sophisticated answers are required for providing remote access as a means of normal operation.

Remote Access - A Structured Approach

ei^3 provides a full suite of Industry Internet of Things solutions that include Remote Access, but also application services that rely on a continuous stream of process data that is collected from industrial machinery in the field. Therefore, ei^3 was faced with the challenge of addressing the "normality" of a continuous data collection in its design from the ground up. With twenty years of experience and the knowledge of thousands of installations in more than 100 countries, our design remains faithful to three basic requirements:

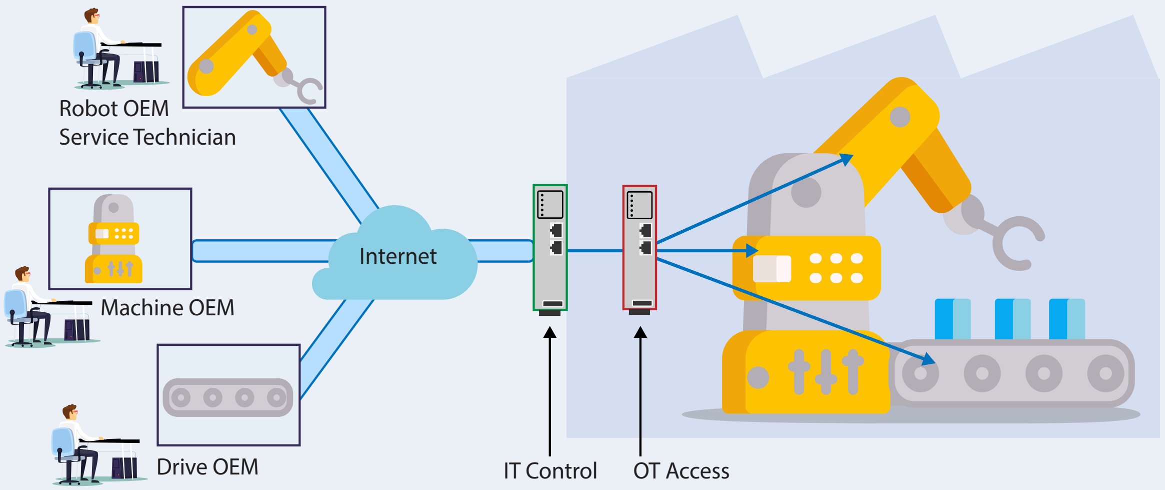


Figure 2

An implementation suitable to support continuous operation must cater for IT and OT requirements, and support a scenario that allow a multitude of users and roles with dedicated access rights to see the system through a unified access point.

1 Ensure "IT" acceptance

The IT department in every organization is responsible for maintaining a data infrastructure that ensures the security and integrity of its corporate data. It is the authority to issue user credentials and access rules that determine who can access what piece of data or digital asset. The IT department determines how remote access is accomplished and is responsible for weighing risks vs. benefits. If data is compromised - for example, confidential information finds its way to a competitor or "Facebook" - the IT department's head is rightfully on the line.

Thus, no IoT or remote access solution can become part of the every-day-fabric of a plant without the acceptance, care, and support of the IT department.

In order to gain IT acceptance, the solution must be:

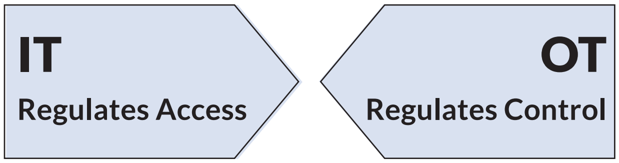
Eminently secure This requires the deployment of security standards that are open, verifiable, and independently audited. This applies to the encryption methodology used when the data is transmitted across non-trusted, insecure links (such as the Internet), but also the user and endpoint-authentication used.

Manageable The IT department must be able to manage network configurations, firewall rules, access rights, as the installation matures and ages. Assets will be moved across networks; network topologies may change or networks may segment, users will be added and removed. Network operators change. The installation has to offer resilience against these changes and the IT department must maintain full managerial and configuration control at all times. Deployments must be possible onto old networks, sometimes with less-than-ideal documentation.

Verifiable The IT department cannot rely only on promises of providers and users. Using their own tools and techniques the IT department must be able to monitor the solution to verify that is it in full compliance with the access policies and data usage that was agreed upon. Closely related to verifiability is **traceability,** which allows actions taken to be seamlessly correlated to results achieved.

Figure 3

IT and OT requirements are sometimes contradictory. A successful remote access implementation will cater for both.



2 Provide “OT” control

In a manufacturing plant, the “Operations Team” is who keeps the production rolling: machine operators, line management, maintenance crews all work together to ensure that the machinery is working at their best, the material is flowing, and quality and quantity targets are met. Typically, the OT team will be the primary user of an IoT solution, employing it to optimize asset utilization, reduce machine downtime, track & trace material and quality parameters, etc. And, of course, use remote access to achieve all of this.

If a line falls short of targets, production is lost and clients walk away – then the OT management’s job is on the line. As such, the OT team will be a critical user of the IoT solution, keeping benefits and risks under close scrutiny.

Giving OT full control over the IoT solution requires:

Fine-grained access control, meaning that any user of the solution must have specific access rights and privileges. The individual machine operator should have full access to his machine, but not other lines. The supervisor should be able to access machine output but may not interfere with technical machine settings. Remote service technicians may be able to view error logs and change settings when requested to do so, but not at other times. Despite of fundamentally different capabilities to see, access, or update machine parts, all users utilize a unified, single control point that provides full control to the OT team.

It is worth noting that even without remote access, outages and production shutdown occur caused not by external but internal activities - operators making mistakes not prevented by control system that are too naive, not to mention disgruntled operators or employees. Good practices around remote access in this regard will naturally also translate to internal access control mechanisms.

Auditability, meaning the OT teams must be in a position to verify any action taken - from process variables being read, to the same being written, to machines being started or stopped - all actions must be accompanied with adequate logging and validation on what authority these actions were executed. This audibility naturally comes with accountability, so that every action and its consequences can be tracked and verified.

Flexibility: Situations that require remote access, data analysis or sharing of process logs may emerge quickly and handling these would require flexible, temporary assignment of rights to remote users.

In many cases the requirements of the IT and OT teams appear to be irreconcilable: the IT teams would prefer to limit access as much as possible whereas the OT teams would like to flexibly hand full control of a machine exhibiting a fault to the service technician of the machine builder half way around the world. In our experience, this potential contradiction of interests can and must be avoided: ei^3 has crafted an overall security and access architecture that has proven to find common ground between both camps, find their acceptance, and has paved the way to highly successful IoT implementations. Perhaps this is due to the third principle that was adopted as a design point.

3 Prepare for the future

Many remote access solutions work satisfactorily for what they have been designed to do - provide remote access in cases of crisis, such as when a machine is down and requires a quick fix applied by a remote service technician. Where they fail is when they are stretched beyond their intended usage scenarios: continuous data collection, remote access as a continuous means of operation, trend and data analysis, etc.

Here, purpose-designed IoT solutions win the day, as they have been designed ground-up for tasks that go beyond situational remote access.

The world is changing.
Covid-19 will pass, and the notion and experience of "social distancing" will be gone eventually. Our approach to work will undergo a lasting transformation: operators and managers who experience the potential of remote monitoring and remote access today out of necessity, will see their clear benefits and will be reluctant to let go of their capabilities in the future.

If you have not yet considered IIoT and Remote Access for your organization, now is the time to do so. If you already have a solution in place, it might be the right time to critically review your installation and see if it is ready for prime time - not just for the odd emergency situation.

About ei3:
ei3's full suite of IoT solutions is built around a continuous data connection to industrial machines and is designed to do so to the satisfaction of the IT as well as OT teams. Leading manufacturers in more than 100 countries have turned to ei3 as their partner of choice since 1999. And while many have started with the notion of remote access, many have since adopted the larger ei3 solution portfolio to manage their production needs.

Ready to assess your remote access solution? Here is our checklist to aid your review:

1 **Does your remote access solution address the requirements of your IT and OT teams?**

ei^{3}'s security architecture is based on a unique two-tier access solution whereby the "gateway" - "Amphion" in ei^{3}'s terminology, is split into two physical components - a single "green" Amphion which facilitates secure data flow to and from the plant from secure data centers, and multiple "red" Amphions which are embedded within industrial assets.

The IT team manages the green Amphion and its connections to the red Amphions. Connections to the red Amphion are open to being verified by the IT teams' conventional "wire shark" protocols, allowing full control of the IoT data traffic and the scope of data collection. The red Amphions are under the control of the OT department, enabling fine-grained control to individual machine components.

Both IT and OT teams use a unified ei^{3} control system to manage users, security credentials, access rights.

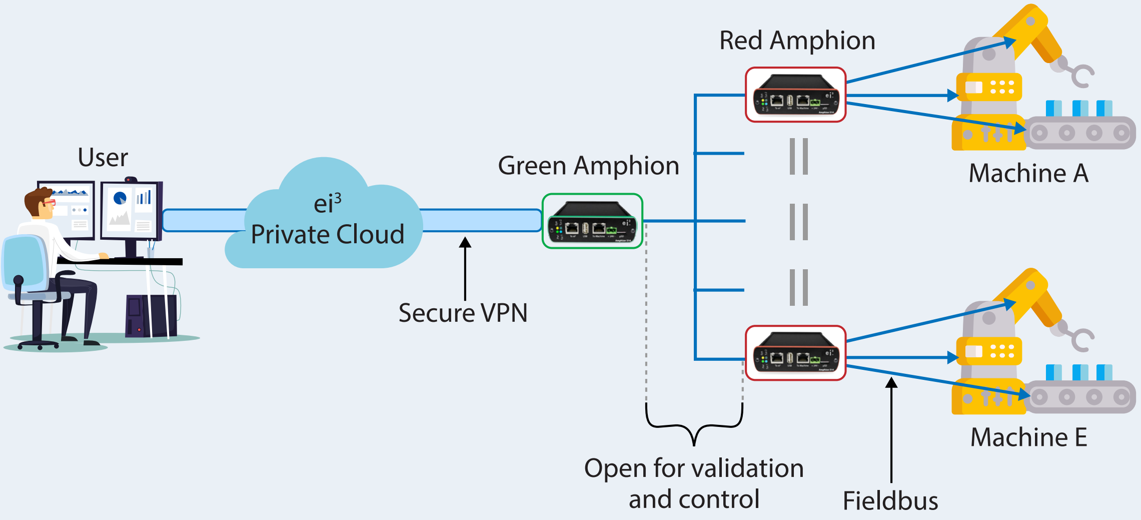


Figure 4

ei3's unique access architecture is based on a two-layer approach that caters for both the IT and OT requirements.

2 Does your solution allow dynamic configuration beyond "One-to-One" connectivity?

ei3 uses dynamic keys that can be assigned to users or groups of users, and are tied to specific roles that come with pre-defined access scope and access rights. These keys may be set up to be long-lasting or may have a time-based expiration date. Keys may also be permanently assigned to specific users.

This takes account of a typical scenario whereby several different parties have different reasons to access a system:

- The PLC vendor may require access to the systems embedded control for software updates and firmware issues.
- The machine builder may access system logs to assess mechanical conditions and assess the need for predictive maintenance.
- The system integrator may access system components for program corrections or modifications.

3 How easy is it to give access to an external expert quickly in an emergency situation?

It is impractical to create thousands of "one-to-one" links for all plant-floor assets, in case expert advice is needed. The ability to link to a specific asset that may need support or external monitoring until an issue is resolved is easy using ei3. If the asset is not already connected to ei3, a red Amphion can easily be added to the device and configured to connect through an existing green Amphion. Since the connection between the red and green Amphions are laid on top of the existing network infrastructure, no modifications are needed at the network level. After that, an access key can simply be sent to the expert by email.

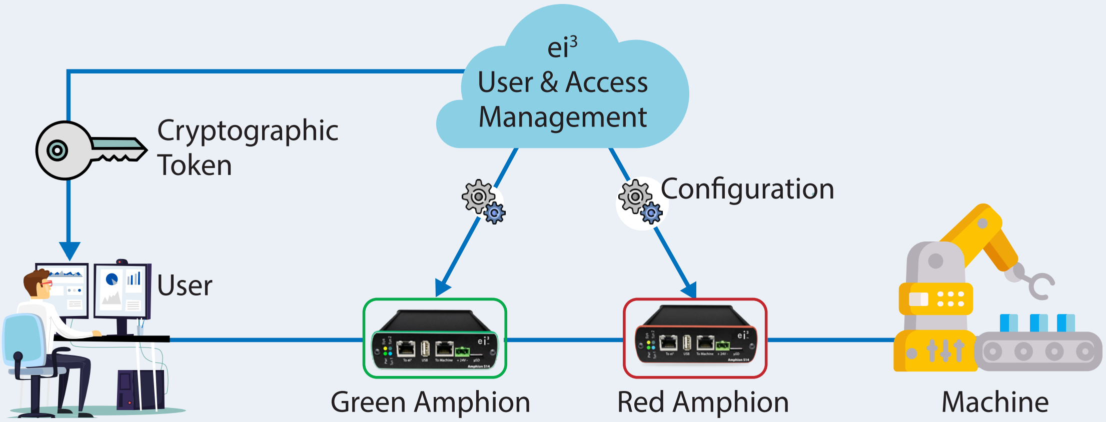


Figure 5

ei3's centralized user and access management functions provide a singular control point to set up users and their specific rights. Cryptographic tokens are used to authenticate the user on entry. These can, for example, be sent to the users by mail or handed over on-line; in any case, the system administrator retains full rights as these tokens can be time-limited, or revoked, at any time, without affecting any other users and their access rights.

4 How easy is it to add your chosen remote access solution to an existing network?

Adding a remote access solution to an existing plant can be tricky as many different generations of network technologies may be deployed, and may not be well understood - unfortunately, not all plants have adopted network standards such as CPwE (Converged Plantwide Ethernet). Upgrading can be costly.

Single point gateway solutions may be a tempting solution due to their perceived simplicity, however this simplicity is gained by full reliance on the underlying network to provide all necessary point-to-point connectivity - potentially requiring complex debugging. If these connections pass through layer 3 switches further configuration management is necessary to ensure rules are set up to enable the required connectivity. These individual connections will become a more significant challenge to manage as more are added or if the network infrastructure is upgraded to its configuration changes.

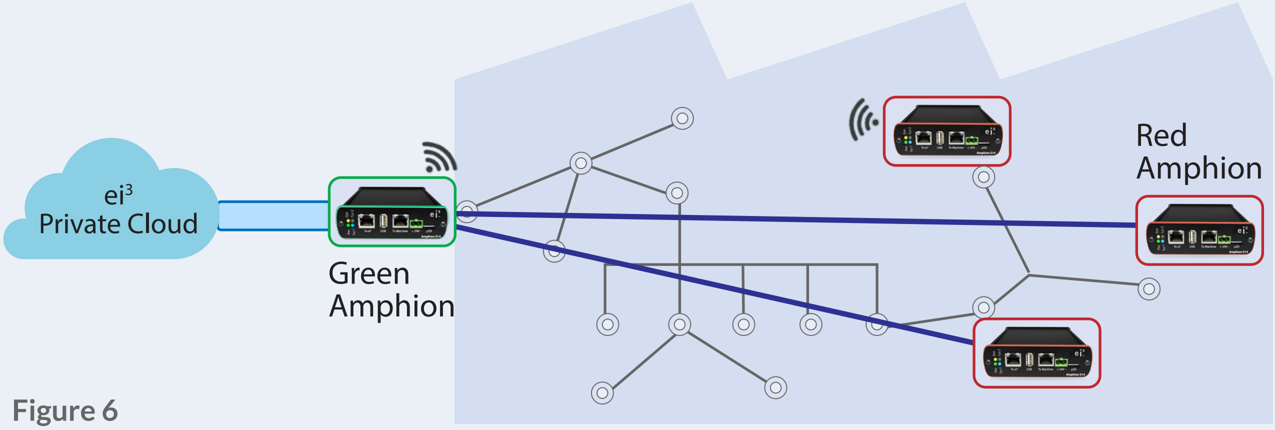


Figure 6

ei3's solution can be deployed as an overlay to existing networks, that may be a mix of technologies, not well documented, and thus not easily extended or changed. ei3's Amphions may establish their overall architecture using existing links where available, dedicated lines where necessary, or even wireless connections where useful.

The ei^3 solution is layered on top of the existing network - this provides a consistent approach regardless of whether the network is based on a set of unmanaged switches or the latest CPwE design. The ei^3 network - consisting of a top-level "Green Amphion" which manages the security of the data to and from the ei^3 data center, and the "Red Amphions" which leads the interaction with each machine asset, is a virtual or actual overlay that can be configured in a number of fashions:

- A VLAN may be used on top of the existing network architecture, allowing all assets and the ei^3 infrastructure components to be grouped within a group of IP addresses.
- A separate physical network may be considered for smaller deployments, ensuring easy configuration, resilience against failures of the corporate network, and offloads the IoT bandwidth requirements onto separate links.
- A wireless network may be considered to support remote assets, or increase deployment flexibility.

5 Can your solution economically scale from one to many assets and users?

Because of the nature of the overlay network, the ei^3 solution scales well by adding additional red Amphion boxes as needed. This is both economical in terms of expense for additional hardware and cost of installation and management.

6 Does your solution of choice provide full traceability by recording all interactions on an individual basis in a centralized log?

Understanding what created a disruption can be challenging. The ei^3 solution creates and stores a history of all activities including invites to remote access. Users are encouraged (and maybe required, depending on the configuration) to add an explanation for their actions to every documented activity. Every single connection, or data access, is logged. The ability to have this archive as part of the solution in which many different companies and individuals participate will allow for transparency and full traceability.

7 Does your solution conform to security standards and has a proven track record to review?

ei^3 solution has proven to be a common ground for IT and OT groups with thousands of clients across the world since 1999. Furthermore, our security models and processes are subject to regular reviews by independent auditors. With this, you can rest assured of the security of our solution compliant to ISO 27001:2013, certified by DEKRA.

Call us for a list of references in your industry.

ei^3 - Certification and Memberships

Information security
ISO/IEC 27001
www.dekra-seal.com
DEKRA
certified

Compliance to
International Standard Organisation (ISO) 27001:2013, certified by DEKRA

Member of
Control System Integration Association

Member of
OMAC,
The Organization for Machine Automation and Control

Member of
MT Connect,
a free, open standard for the factory

ei^{3} Corporation
Tel. +1 201 802 9080
E-mail: contact@ei3.com
Website: www.ei3.com

Contact us so we can help you as you develop your plans for providing remote connectivity.

With over 20 years of experience, ei^{3} is in a unique position to provide a vendor-agnostic, scalable, and comprehensive solution that is IT approved and OT Managed — delivering the ROI of the Industrial IoT from day one.