Access your data without exposing your network

WHITE PAPER

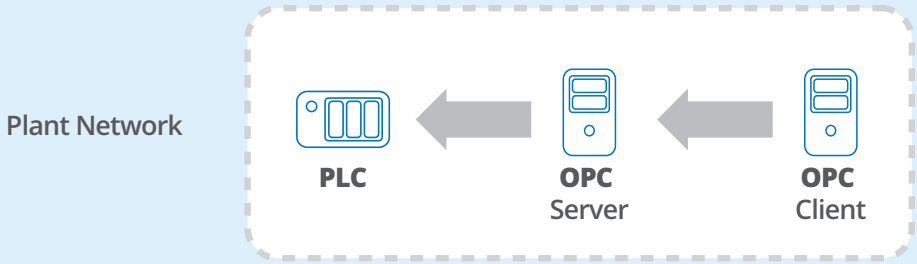
Secure remote access for Indusrial IoT and Industrie 4.0

Industrial IoT and Industrie 4.0 present a fundamental security challenge. On the one hand, connecting outside the plant network was never contemplated when industrial systems were first being designed, because the need did not yet exist. On the other hand, IIoT and Industrie 4.0 requires making connections to industrial systems, be it in-house from corporate IT networks or from remote locations via the Internet. This need to access industrial data raises the question: What is the best way to maintain the high level of security that mission-critical systems require, while allowing remote access to the data?

Traditional Client-Server Architecture

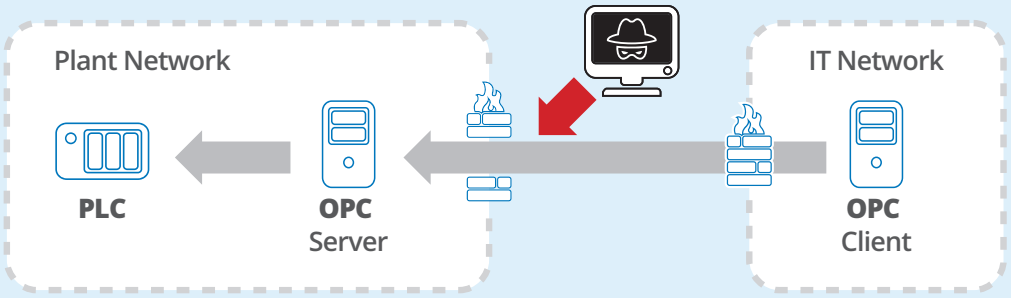
This basic problem highlights the need for a new, secure, design approach for IIoT and Industrie 4.0. Until now the architecture for most control systems, such as those used in factories and on pipelines, assumed that they were running within a secure perimeter. Firewalls, DMZs, and sometimes even air-gapping have been used to ensure that nobody can access the plant network from outside. Within this perimeter, plant networking typically connects PLCs and other devices to SCADA systems, HMIs, and other clients using industrial protocols like OPC. In this self-contained world, OPC servers connect to PLCs to gather their data. Then OPC clients like historians, HMIs, or SCADA control panels connect to the OPC servers to access that data. The process and its data are secure as long as the network is closed off from the outside world.

 • 2233 Argentia Road, Suite 306 • Mississauga, ON L5N 2X7 • +1.905.702.7851 • info@skkynet.com



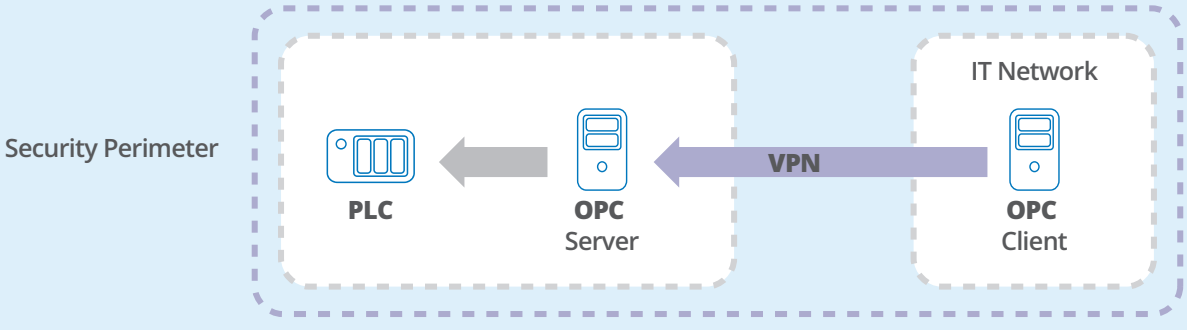
Access from other locations

The traditional architecture works fine within the security perimeter of the plant. But what happens when someone wants to access plant data from another location? Putting a remote OPC client outside the plant (say, on the IT network) and connecting to the OPC server inside the plant requires opening a firewall port on the plant network. This exposes the network to attack, and is a serious security concern.



Why not use a VPN?

One solution that may come to mind is to use a VPN (Virtual Private Network). However, a VPN won't actually solve the security problem. A VPN effectively extends the security perimeter beyond the plant network to include the IT network. This expands the attack surface to both networks. Worse yet, a security breach on the VPN will expose all systems on both networks to attack. Instead of just sharing the process data, a VPN shares the whole network.



The highly publicized attack on the Target chain of stores in the USA is a good example. A contractor who was given VPN access to the company system was the victim of a phishing attack. With access to the contractor's system, the attacker found the necessary VPN credentials to then enter the Target system. He quickly found his way to customer records and credit card numbers and had a field day.

In the same way, a VPN would not have protected an industrial system from the WannaCry attack. That virus arrived by email and then unloaded a "worm" that attacked all of the computers on the network. Any attacked computer that was logged onto a VPN would have automatically infected all the others.

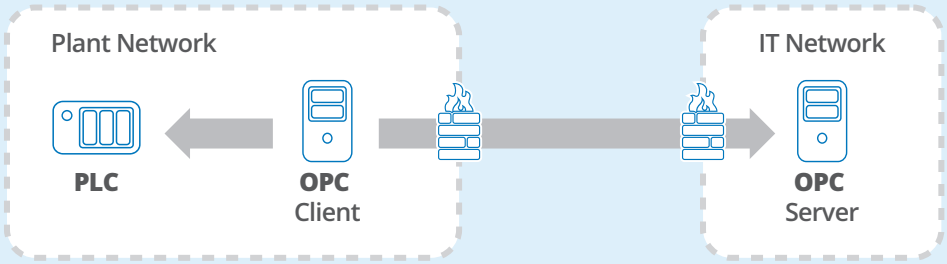
The drawbacks of using a VPN for industrial applications are examined in detail by Clemens Vasters, a Microsoft Developer. In a paper titled Internet of Things: Is VPN a False Friend? Vasters said, "VPN provides a virtualized and private (isolated) network space. The secure tunnels are a mechanism to achieve an appropriately protected path into that space, but the space per-se is not secured, at all. It is indeed a feature that the established VPN space is fully transparent to all protocol and traffic above the link layer."

Why not reverse the connection?

The problem of the open firewall port is due to the inbound connection to the plant. This vulnerability could be overcome if there were a way to make the connection outbound instead of inbound. So why not switch the client and server locations? In a client/server relationship, the connection is always initiated by the client, so to make an outbound connection you could put the client inside the plant, connecting outwards to the OPC server, which would be on the IT network.

This would provide an outbound connection, but no data. The client must get its initial data values and updates from the server. If the server is not on the plant network and not connected to the data source, it cannot provide that information.

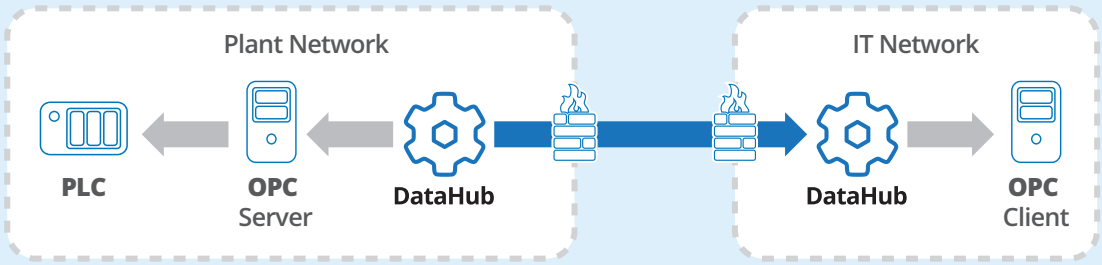
Although it doesn't work to simply switch the positions of server and client, making an outbound connection is still the most secure approach. Is there any other way to do it?



A different kind of outbound connection

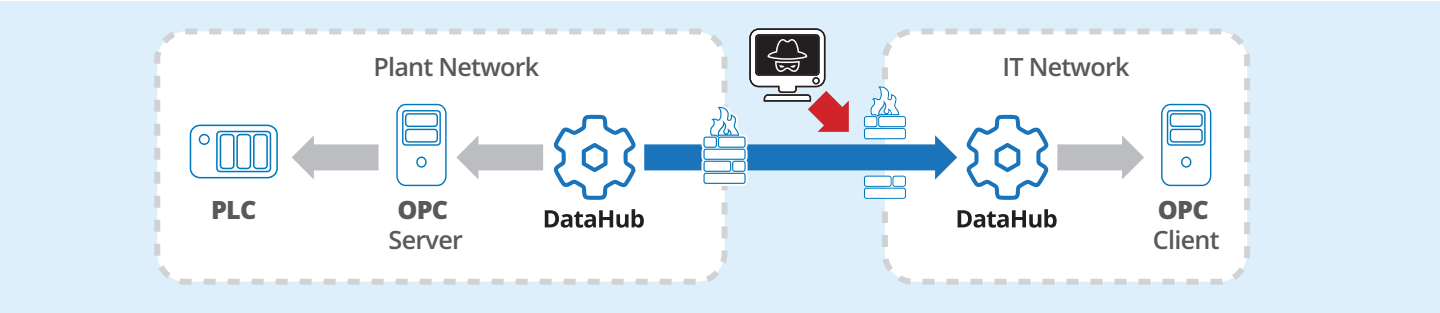
The Cogent DataHub® is flexible in how it makes connections. When one DataHub connects to another DataHub, either one can initiate the connection, and either one can be configured to be the trusted, authoritative data source. (By "authoritative" we mean the side of the connection that has the correct data in case of a disconnect/reconnect on the network.)

The ability to assign the trusted data source and who makes the connection resolves the client/server problem, because now the authoritative source of the data can also initiate a connection. Thus, by putting one DataHub on the plant network and another DataHub at the remote location, you can make an outbound connection from the plant network, and still maintain the correct authority for the data.



This fundamental difference from the traditional server/client relationship is the foundation of Skkynet's secure-by-design software and services for IIoT and Industrie 4.0. Making only outbound connections using the DataHub keeps all the plant firewalls closed, and protects the plant network from attacks.

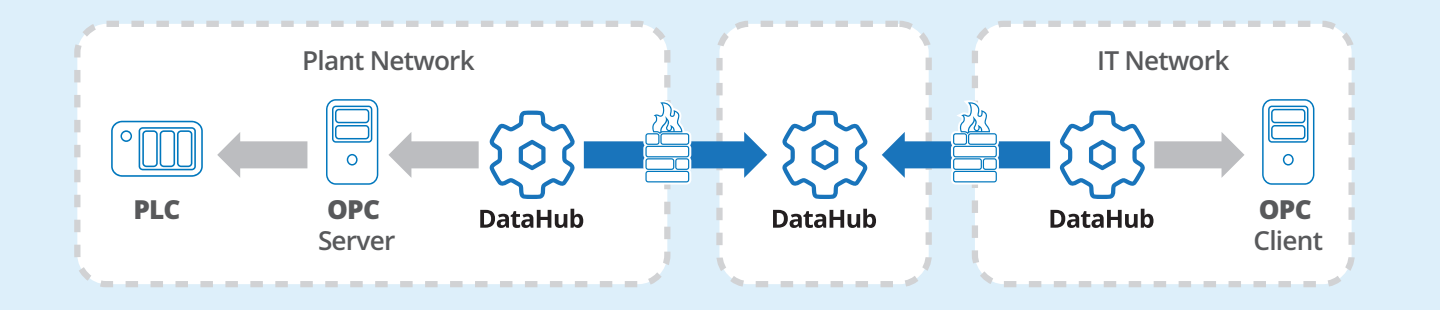
Depending on your security requirements, this may be all that is needed. But there is more to the story. Although the plant network is protected, the remote location must now open a firewall, exposing it to attacks.



Ideally, all the connections, be they from the plant network, the IT network, or any other remote client should be outbound only. This locks down the firewall on both networks, presenting no attack surface.

Secure Middleware

The server and client systems can be secured by placing another DataHub in the middle which accepts incoming connections and brokers the exchange of data between the source and the user.



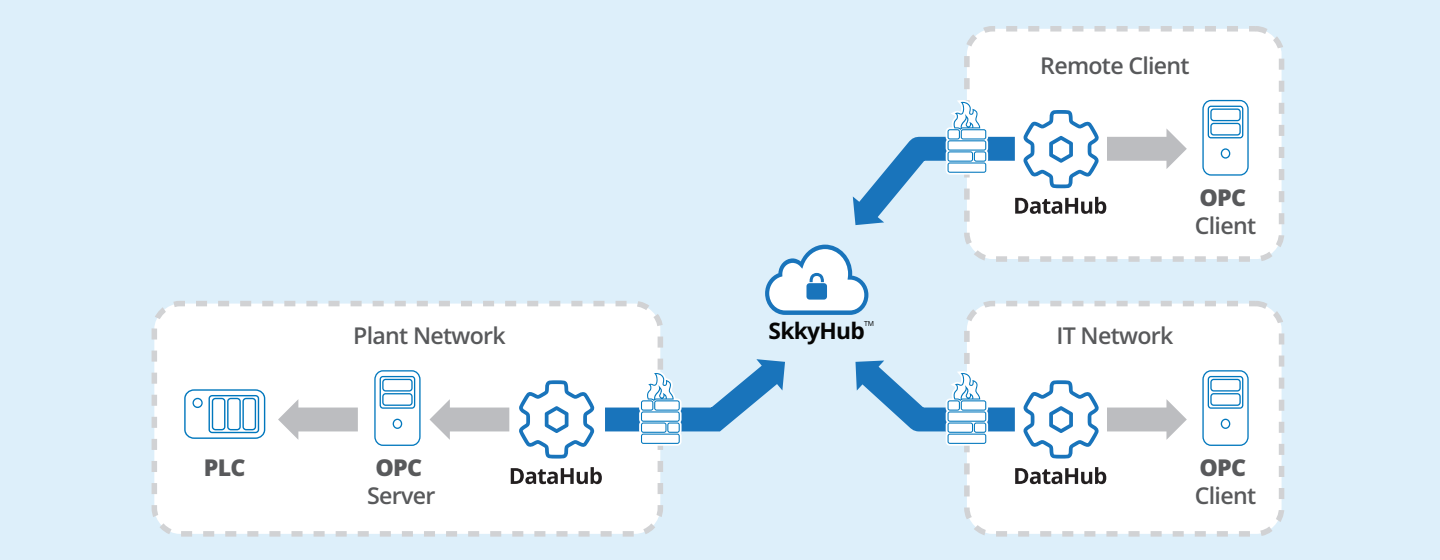
In this way, both the plant and IT networks make only outbound connections. At the same time, because each DataHub along the communication chain from source to user is configured separately, each link in the chain becomes a trusted, authoritative source of data. Thus, if any part of the network goes down, the client is informed, and when the connection is re-established, it gets updated with the latest, trusted data from the source.

With all firewalls closed on both the plant and IT networks, the potential attack surface for the system has now moved to the DataHub in the middle, reducing the complexity of the security problem. The central DataHub can now be hosted on a secure DMZ computer that can be configured to manage the security risk. The DMZ could run on the corporate network or on a private cloud system.

Cloud Service

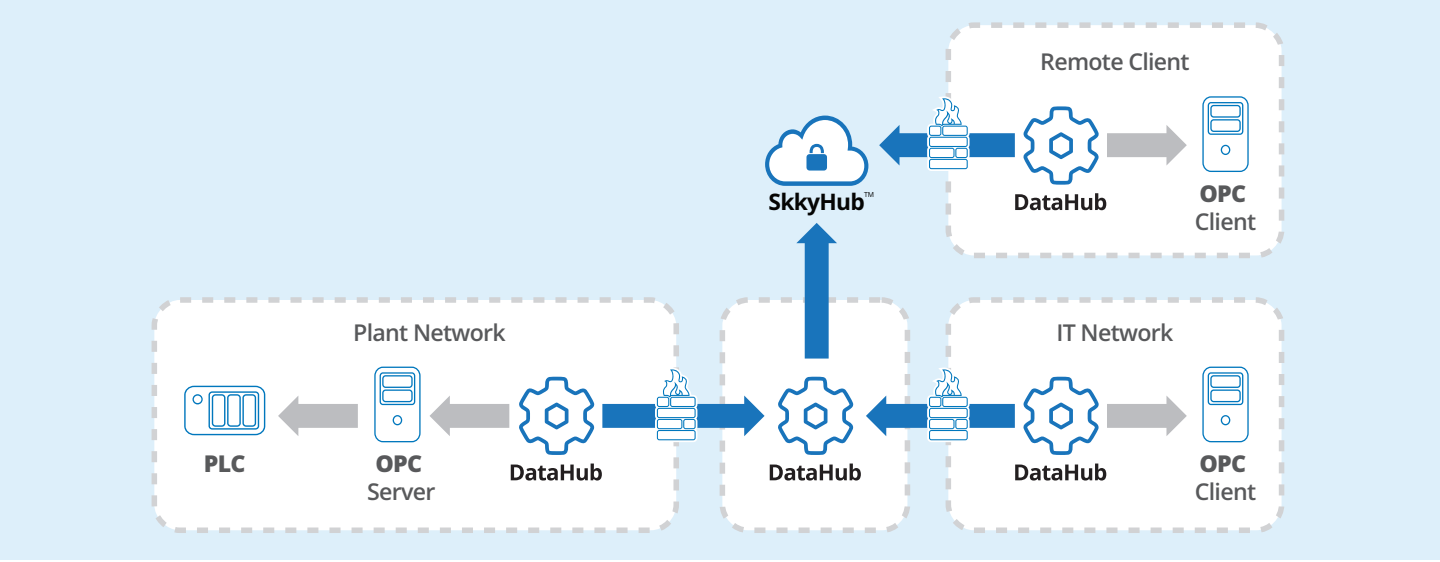
As an alternative to using a local DMZ, the SkkyHub™ service provides a fully hosted DataHub in a DMZ running in the cloud. With SkkyHub, plant data can be safely shared with remote users, eliminating the uncertainty of 3rd-party connections to a local DMZ or plant network. In fact, the SkkyHub service can even replace the local DMZ altogether, saving resources and providing secure outbound connections for the plant and IT networks.

The SkkyHub service offers secure data connectivity and integration that makes it easy to connect and network virtually any industrial system or embedded device. It accepts inbound connections from the DataHub and provides a built-in Web-based HMI, allowing users to monitor or control their process or device from almost anywhere, with no programming necessary.



Hybrid Cloud

Finally, it is also possible to combine a local DMZ-based solution with SkkyHub to create a hybrid cloud service. This provides robust local networking via the DMZ server as well as secure, outbound connectivity to the cloud for remote access to the data. Should the Internet connection go down, the IT network would stay connected.



Share your data, not your network

Any of these four approaches: making secure outbound connections with the DataHub, or using a DMZ, or SkkyHub, or both in a hybrid cloud provides the same, DataHub-based, secure access to process control data, with no VPNs and no open firewall ports on the plant network. The DataHub and SkkyHub secure-by-design architecture lets you share your data, not your network. This is how to keep mission-critical systems secure, while participating fully in Industrial IoT and Industrie 4.0.

About Skkynet

Skkynet Cloud Systems, Inc. is a global leader in real-time data communication systems, providing the award-winning SkkyHub™ service, DataHub® middleware, and Embedded Toolkit (ETK) software, which enable secure, real-time data connectivity for industrial automation, Industrial IoT, and Industrie 4.0. For more information, see https://skkynet.com.

 • 2233 Argentia Road, Suite 306 • Mississauga, ON L5N 2X7 • +1.905.702.7851 • info@skkynet.com