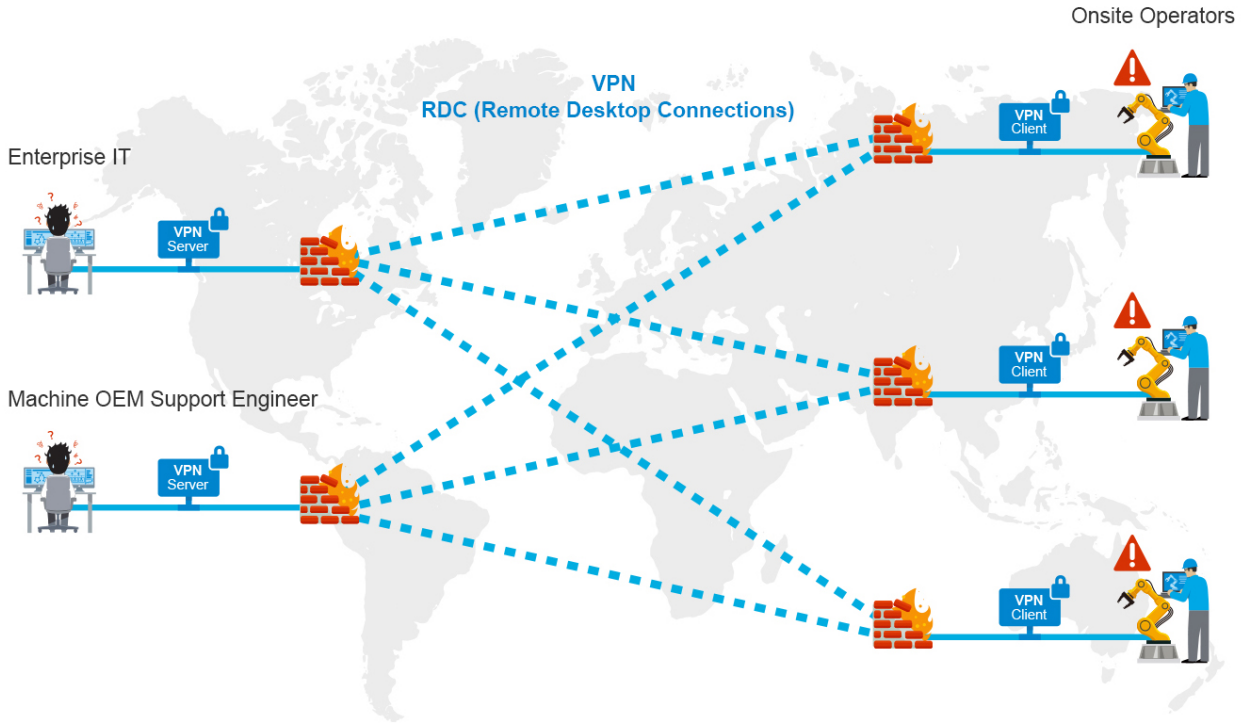
Simplifying Connectivity for Mass Customization

Mass customization allows manufacturers to meet customer expectations for products built to their exact specifications within an even shorter amount of time. In order to reduce system downtime in a fully automated mass customization manufacturing process, it is necessary to be able to efficiently upgrade, troubleshoot, and maintain more connected machines from remote distances. We look at ways to simplify connectivity for you to enable secure and reliable networks.



With the advent of the Industrial Internet of Things (IIoT), mass customization has strongly positioned itself as the new frontier in manufacturing industry due its potential to help companies increase earnings and gain a competitive edge. In short, mass customization conveniently pairs the offering of customized goods with the benefits of mass production. To tailor production output of customized products on a large scale, mass

customization requires leveraging flexible computer-aided manufacturing systems, which essentially allow programmable robotic systems
to switch between models and variants without losing time and compromising productivity.

It?s All About Reliable Data Transmissions

To ensure smooth operations and on-time deliveries, data integrity and consistency are key. For
the largest home appliance manufacturer in China, for example, connecting reliable production
data in interconnected factories has been fruitful for their mass customization strategy. The
manufacturer enhanced its production efficiency and flexibility by leveraging the power of a
connected ecosystem. Network availability was ensured by combining industrial-grade hardware,
providing redundancy protocols, with network management software. As a result, a reliable and
secure connection to the manufacturing systems allows orders to be customized, logistics to be
further automated, and customers to check the status of their orders. Furthermore, as real-time
data is supplied from the shop floor, production managers can monitor the production line more
effectively and tackle any issues well before full-blown problems arise.

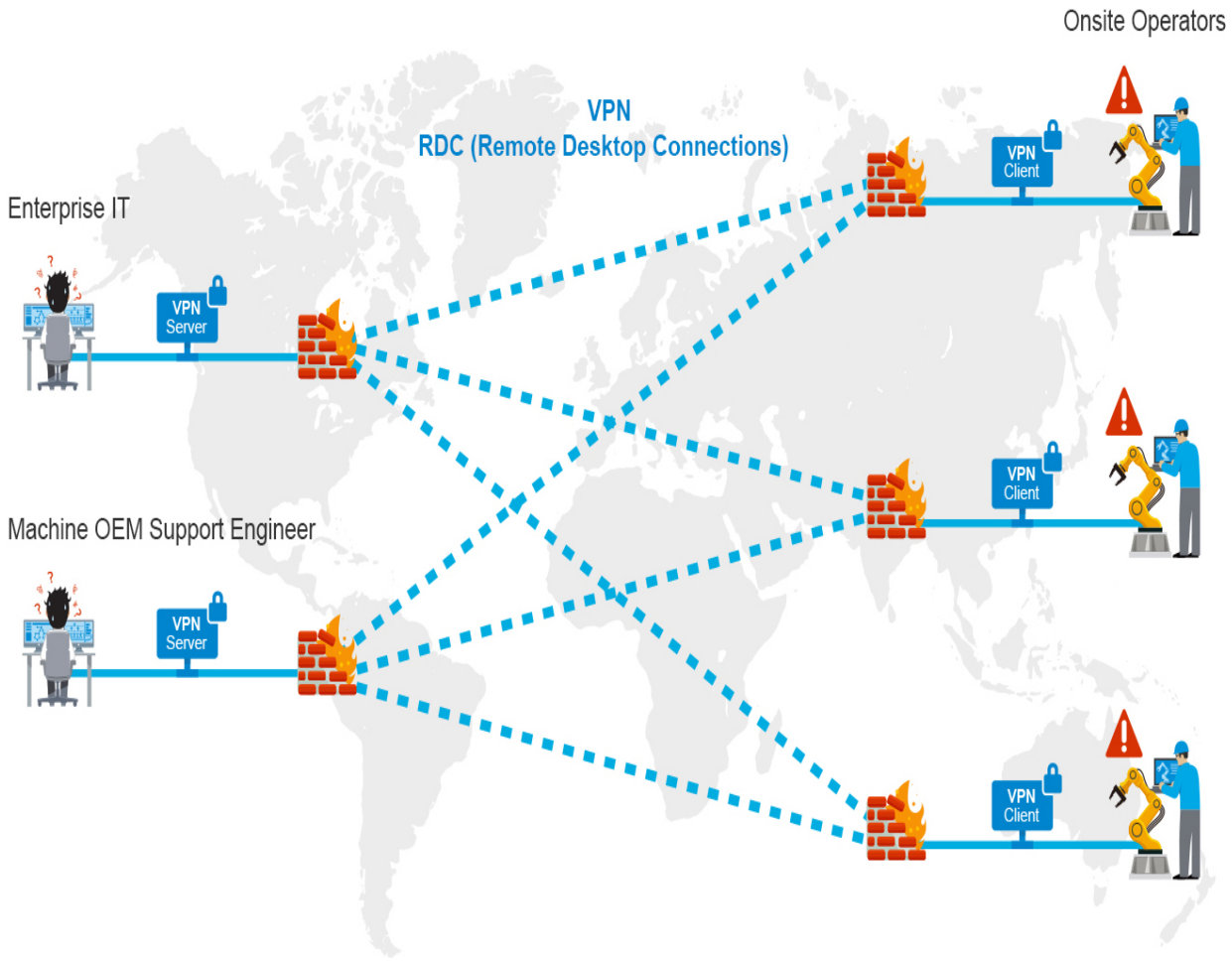
The Stumbling Blocks to Connecting to Mass Customization

Manufacturers have come to lern that two challanges stand between them and mass customization connectivity: the large amount of time
spent to establish multiple scure access and overcoming security silos for interconnected systems. in order to further reduce system downtime
in a fully automated mass customization manufacturing process, it is necessary to be able to efficeniently upgrade, troubleshoot and maintain
more connected machines from remote distances. Adiditonally with more IT system connected to individual control systems (ICS),
manufacturers also need to protect all these newly interconnected machnies and industrial subsystems from internal and external threats. For
the purpose of this article, we will focus on establishing mulitple secure access effortlessly.

VPNs and RDCs Are Not Always the Answer

Remote access allows users to administer and even control machines within a corporate netwrok from distant field sites. Granting remote access to multiple devices offers many benefits for manufacturers, such as the ability to monitor multiple plants without the need for travel or on-site staffing. Upgrades and troubleshooting can also be performed from afar, which can reduce the cost and time needed for maintenance and keep system downtime at bay.
Although virtual private network (VPN) and remote desktop connection (RDC) technologies are commonly used methods for granting remote access to company machines and equipment from field sites, a number of problems are associated with VPN or RDC deplyments for large-scale manfacturing applications.

- Deploying a large-scale VPN requires extensive IT knowledge and skills to establish encrypted layered tunneling protocol connections. In order to secure the private connections that allow remote users to access enterprise resources and applications, user authentication methods, including passwords and certificates, also need to be used and properly managed. All of these requriements can make VPNs especially time-consuming and costly to deploy at large scale.
- As RDC applications need to bypass certain corporate security policies, malicious actors can exploit seemingly legitimate remote desktop sessions to gain unauthorized access or control company resources. In large-scale networks, the risks are compounded by the number of remote desktops connections



Making Large-scale Secure Remote Access Easy

To simplify large-scale remote access, solutions require ease of use, enhanced security, and flexibility to enable users at remote sites to securely access and control coputers, machines, and other industrial equipment located within the factory environment.

As users want to avoid complex technical configurations, plug-and-play remote access brings ease of use to the solution. With a remote access connection that is centrally monitored and managed from a secure cloud server, virtual IP addresses make multiple remote access effortless by eliminating the need to manually reconfigure IP addresses for field devices

For enhanced security, the ideal solution will provide VPN-based point-to-point encryption. Companies can grant on-demand remote access and control that conform to their exisitng IT security policies and enable remote connectivity without having to compromise network protection.

With regard to flexibility and scalability, a solution hould allow users to remotely access and control equipment, as if they
were locally connected, in different connection scenarios, including one-to-one, one-to-many-many-to-many, and site-to-site

Moxa´s Solutions

Moxa Remote Connect (MRC) provides an easy-to-use, secure and fleixble cloud-based solution for large-scale remote access. MRC is perfect
for large-scale deployments because it only requires threee components--the MRC gateway, a cloud server and client software for both desktop
and mobile devies- to enable users at remote field sites o securely access and control computers,machines and other industrial equipment
located within the factory environment.

