Application Note Part 3

Simplifying Connectivity for Mass Customization

Secure remote access and holistic security for interconnected industrial control, IT, and OT subsystems are essential to achieve uninterrupted mass customization in a fully automated manufacturing process

Mass customization, which entails leveraging flexible computer-aided systems to tailor production output on a large scale, has emerged as a key strategy for helping manufacturers maintain market share in the age of Industry 4.0. These flexible manufacturing systems allow output to be customized at item level on a massive scale. What's more, mass customization allows manufacturers to meet customer expectations for products built to their exact specifications within an even shorter amount of time. Within this context, data integrity and consistency are imperative to ensure smooth operations and on-time deliveries.

In order to further 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. Additionally, with more IT systems connected to industrial control systems (ICS), manufacturers also need to protect all these newly interconnected machines and industrial subsystems from internal and external threats. Find out how the following two challenges to connectivity block your way to connect to mass customization.

Case in Brief:

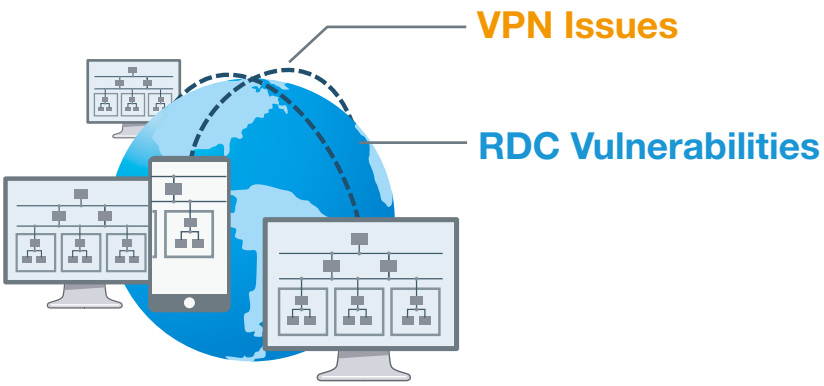
Connecting Reliable Production Data in Interconnected Factories

The largest home appliance manufacturer in China uses Moxa's solutions to enhance production efficiency and flexibility by leveraging the power of a connected ecosystem. Industrial-grade hardware that provides redundancy protocols is combined with network management software to ensure network availability and health. A reliable and secure connection to the manufacturing systems also allows orders to be customized, logistics to be further automated, and customers to check the status of their orders. Also, 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. Learn More

Establishing Multiple Secure Access Is Time-Consuming

Remote access allows users to administer and even control machines within a corporate network 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. In fact, "60 to 70% of machine problems require a simple fix, such a software upgrade or minor parameter changes – which can be done remotely" *(Plant & Work Engineering Magazine)*.

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 deployments for large-scale manufacturing applications:



VPN Issues

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 requirements can make VPNs especially time-consuming and costly to deploy at a large scale.

RDC Vulnerabilities

Although it is generally easier for remote desktop applications to enable simple one-to-one remote control of corporate desktops from another computer over the Internet, RDC applications also need to bypass certain corporate security policies. This allows malicious actors to 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 desktop connections.

WHAT IF

We Can Simplify Large-Scale Secure Remote Access?

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

Ease of Use

MRC provides plug-and-play remote access without the need for complex technical configurations. The remote access connection is centrally monitored and managed from a secure cloud server, and virtual IP addresses make multipoint remote access effortless by eliminating the need to manually reconfigure IP addresses for field devices.

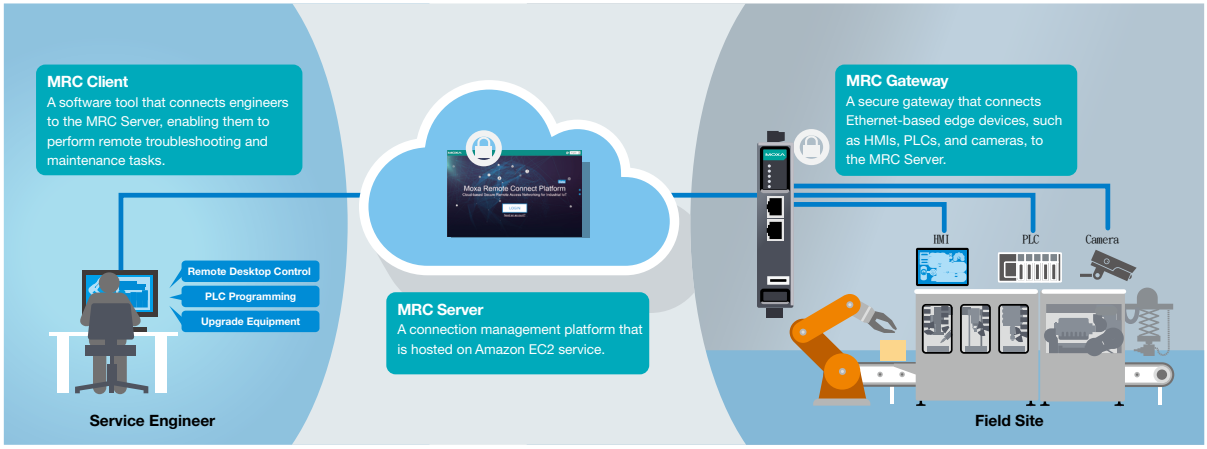
Enhanced Security

MRC protects against man-in-the-middle attacks, data loss, and other security threats by providing VPN-based point-to-point encryption. With MRC, companies can grant on-demand remote access and control that conform to their existing IT security policies and enable remote connectivity without having to compromise network protection.

Flexibility and Scalability

MRC allows 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. What's more, the MRC client software can be installed on any laptop of an authorized maintenance engineer, allowing for even greater flexibility when controlling remote desktops, upgrading equipment, or programming PLCs from afar.

Our Solutions



Overcoming Security Silos for Interconnected Systems

Traditional industrial control system (ICS) networks are physically isolated and not directly connected to the Internet. Although isolated networks are relatively immune to cyberattacks, fully automated mass customization requires interconnected systems that may be exposed to internal and external threats, presenting new challenges to existing IT and OT teams. Technologies and practices used by IT and OT were originally designed for different purposes, and information silos between these disciplines are common. Besides breaking down the barriers between these disciplines, manufacturers face a number of challenges when it comes to securing newly interconnected industrial control systems and converged IT-OT subsystems.

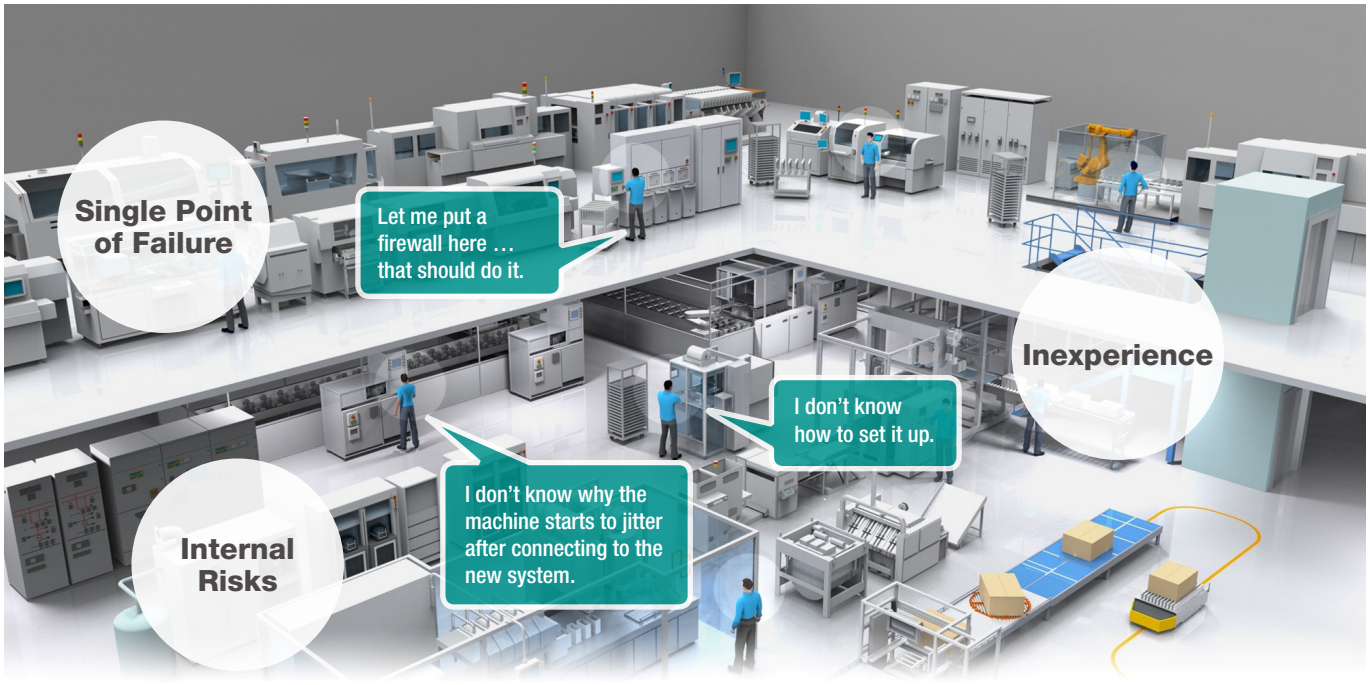


Figure 1: Three issues of mass protection

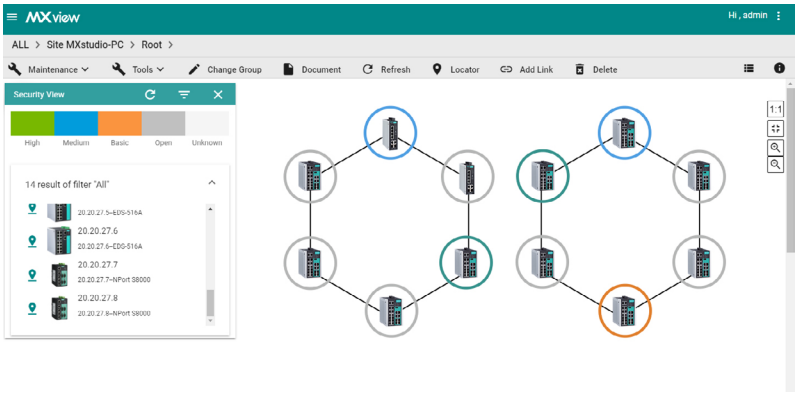
- **Single point of failure:** A chain is only as strong as its weakest link. Connecting formerly independent systems to the Internet exposes ICS networks to new cybersecurity risks. Legacy ICS networks often still lack systematic security protection because their former isolation provided a degree of immunity from network threats. Once connected to the Internet, their vulnerabilities could be easily exploited to undermine overall system integrity.
- **Inexperience:** Integrating IT and OT requires IT system know-how and OT domain knowledge. New security technologies may inadvertently affect IT, OT, or both landscapes, and lead to disruptions in the production line if both sides of the equation are not sufficiently prepared.
- **Internal risks:** Even after converging IT and OT subsystems, information silos may persist and manifest themselves as interferences or communication failures when multiple domains or subsystems are involved in a process or task.

WHAT IF

We Can Simplify Your IT-OT Security Collaboration?

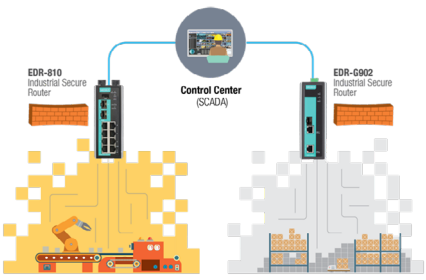
Moxa provides a triple-layer security architecture that allows IT and OT departments to deploy a complete cybersecurity infrastructure that collaboratively incorporates company-wide security policies, operational risk management, and asset performance. Rest assured that your interconnected and Internet-connected ICS networks are safe with Moxa's cybersecurity protection based on ISA 99/IEC 62443 standards.

- **Security management:** Moxa's MXview network management software provides visualized management for security auditing and monitoring. The Device Inventory Report allows you to automatically discover and track the devices on your network. If devices are compromised, you can use the Configuration Center and ABC-01/02 Backup Configurator to back up and restore configurations. You can also use the Security View or Security Wizard to check if device settings meet your company's security policies. What's more, the Real-time Security Events & Logging function and SNMP & RESTful API Northbound Interface allow you to log events to monitor security policy breaches.

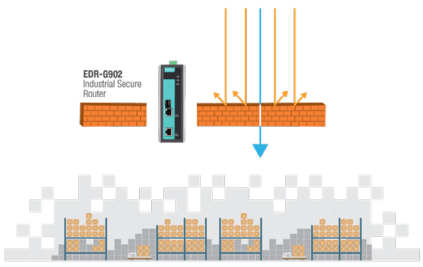


- **Secure network infrastructure:** Moxa's defense-in-depth protection for industrial control systems covers network segmentation, secure data communication and filtering, and secure remote access. Prevent breaches from crashing the whole system by using industrial firewalls to segment the network into secure cells or zones, or by using network address translation (NAT) to segment public and private IP address ranges. Use industrial firewalls that support Modbus deep packet inspection (DPI), DoS protection, and access control lists (ACL) for secure data communication and filtering. For secure remote access, Moxa Remote Connect provides a secured, flexible, and scalable remote VPN-based management platform for secure communication over public Internet connections.

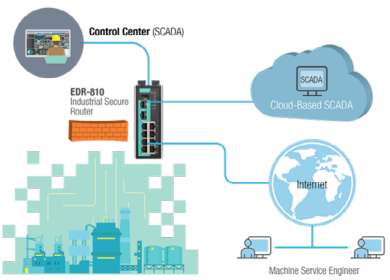
Network Segmentation



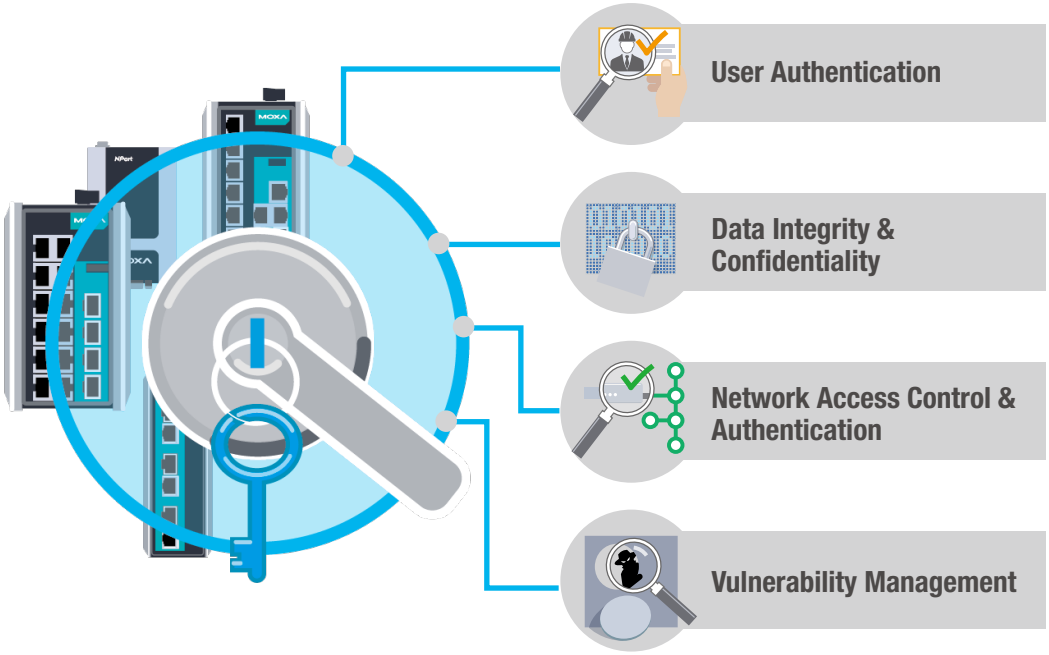
Secure Data Communication and Filtering



Secure Remote Access



- **Device security:** Last but not least, Moxa provides hardened devices with embedded security functions. These features authenticate the users that log onto your devices, encrypt connections to devices for configuration and management, verify which devices are permitted to access the network and communicate with other devices, and enable a well-defined process for responding to network vulnerabilities.



Our Solutions:

- Defense-in-depth cybersecurity that includes secure devices, secure network infrastructure, and security management.