How to Mitigate Cyberrisks While Maintaining System Availability

Risk 1

If you do not have a full understanding of your industrial network status you may not be able to respond quickly or effectively.

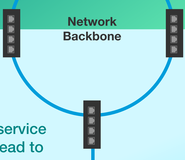
Supervisory Network

Risk 2

Even though a north-south bound firewall has been implemented, unauthorized network access through third parties may still happen.

Industrial Ethernet switches

Risk 3



Leaving unused service ports open may lead to a DoS attack.

Read the checklist for your industrial network security.

Risk 4

That is why you need an industrial IPS.

Unauthorized devices may implant malware into the HMI which then spreads across the network.

Risk 5

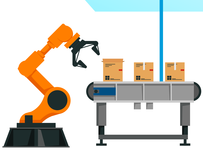
Most serial data communication (proprietary protocols) are not encrypted, leaving the communication unsecured and open to exploitation

Check out the device security solutions.

Risk 6

Security patches are not available or feasible for PLCs.

That is why virtual patching is important.



Mitigating vulnerabilities and securing your industrial networks are our first priority.

Visit www.moxa.com/Security for more information.

www.moxa.com