



TOP RECOMMENDATIONS FOR SECURE REMOTE ACCESS TO INDUSTRIAL CONTROL SYSTEMS

**FPSA Technology Network would like to recognize
HMS Networks for their efforts in developing this tech
note resource.**



In the market looking for a vendor to provide networking services?

Please visit HMS Networks at www.hms-networks.com.

To learn more about our best-in-class solutions, which meet these recommendations, please visit <https://www.ewon.biz/products/cosy>.

Preamble

Using the Document

This document is intended as recommendations for End Users for the requirements to allow secure remote access to machines and other Industrial Control equipment by vendors.

TOP RECOMMENDATIONS FOR SECURE REMOTE ACCESS TO INDUSTRIAL CONTROL SYSTEMS

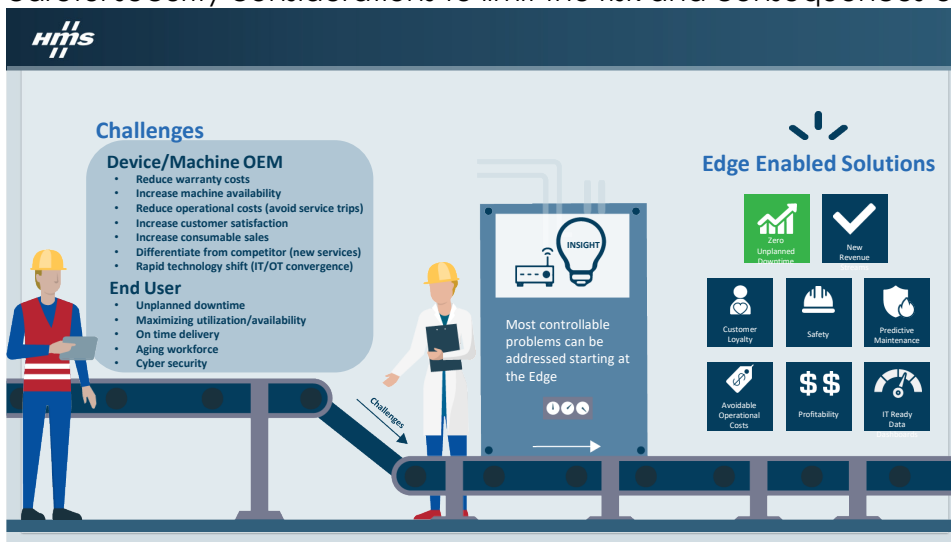
1. Why Remote Access

Remote access grants the ability to remotely connect to intelligent devices, such as PLCs, HMIs, or robots, with similar functionality as if onsite. The resulting cost savings and ability to act immediately when a machine fails will help to ensure machines are working at their maximum level of productivity.

Remote access to machines for vendor support brings clear advantages to manufacturing: 63% of the maintenance work on a machine is for a routine check or simply no problem (source: ARC Advisory Group). The average cost per hour of downtime in some factories, such as pharmaceutical or automotive, might exceed 1M USD* (Source: IT Performance Engineering and Measurement Strategies: Quantifying Performance and Loss, Meta Group, Oct. 2000)

The use of public networks for accessing industrial plants or machines leads to possible threats in the form of cyberattacks over the assets exposed on the Internet. An attack on one industrial control system might have undesirable consequences such as interfering with the process operations, changing the programs of the PLCs without authorization, sending false information to operators, or inhibiting alarm conditions, among others. Even though PLCs and industrial protocols have been considered for hackers to be "obscure" systems for years, getting information about how to reach them is relatively easy to find. Therefore these threats are becoming a bigger risk.

Remote access can provide clear advantages for a business, but it must be done with careful security considerations to limit the risk and consequences of a cyberattack.



2. About Industrial CS

There are important differences between how Industrial Control Systems work and IT (Information Technologies) systems, which lead to a specialized approach on handling security. Industrial Control Systems use proprietary operating systems designed to work at

TOP RECOMMENDATIONS FOR SECURE REMOTE ACCESS TO INDUSTRIAL CONTROL SYSTEMS

nearly 100% uptime, with a Fieldbus connected to real inputs issued by sensors or output for control. These discrete controls use protocols for efficient high-speed data transmission and deterministic processes but not for security. Priority in the design of an Industrial Control System is availability.

Although many of the standards and best practices for IT security are valid for the Industrial Control, additional considerations must be given, especially because the concept of risk and priorities in Industrial Control systems differ from those of the IT world. While a Risk Analysis for IT would consider the impact on possible data loss or business operations failure, Industrial Control Systems consider first the risk of life, equipment, or product loss.

Therefore, priorities are also different: IT (Information technology) security focuses on the confidentiality of the information, whereas in OT (Operational technology), the system's availability is the focus.



Other key differences in the requirements can be summarized as follows

IT	OT
Non-Real Time	Real-time
The response must be reliable	The response is time critical
High throughput demanded	Modest throughput acceptable
High delay and jitter accepted	High delay is a serious concern
Occasional failures tolerated	Outages intolerable
Data integrity paramount	Human safety paramount

Availability and safety are the top two priorities in manufacturing, even over security. Both can sometimes conflict with security in the design and operation of any control system.

Guidelines and standards are available for industrial cybersecurity, such as IEC62443, NIST SP800, and ISO27001, among others.

TOP RECOMMENDATIONS FOR SECURE REMOTE ACCESS TO INDUSTRIAL CONTROL SYSTEMS



3. ARCHITECTURE FOR SECURE REMOTE ACCESS

When considering a remote access system, the electronic security perimeter is difficult to qualify due to the responsibility of the remote access security remaining on the vendor side (normally outside of the trusted zone); the vendor has to provide adequate countermeasures for Remote Access. In many cases, the machine vendor will assign all manufactured machines the same Ethernet parameters – i.e., the same IP address – and the same VPN server. If an end user provides the IP addresses that match his plant configuration, they would have access to significant portions of the network, which are then considered unauthorized. If the end user utilizes a specific VPN technology provider, the machine builder would have to install a custom VPN client on every PC. This would increase the complexity and costs associated with design, build, and installation.

To overcome these limitations, HMS proposes a modern cloud-based solution for providing services for secure Remote Access services. These services connect users to their machines via the Internet. Users are typically Service or Automation engineers who need to access their machines installed on several customer premises, usually spread worldwide.

A software application running on a PC is installed on the user side. This software application establishes a seamless communication link between the PC and the cloud service through the Internet at the user's request.

TOP RECOMMENDATIONS FOR SECURE REMOTE ACCESS TO INDUSTRIAL CONTROL SYSTEMS

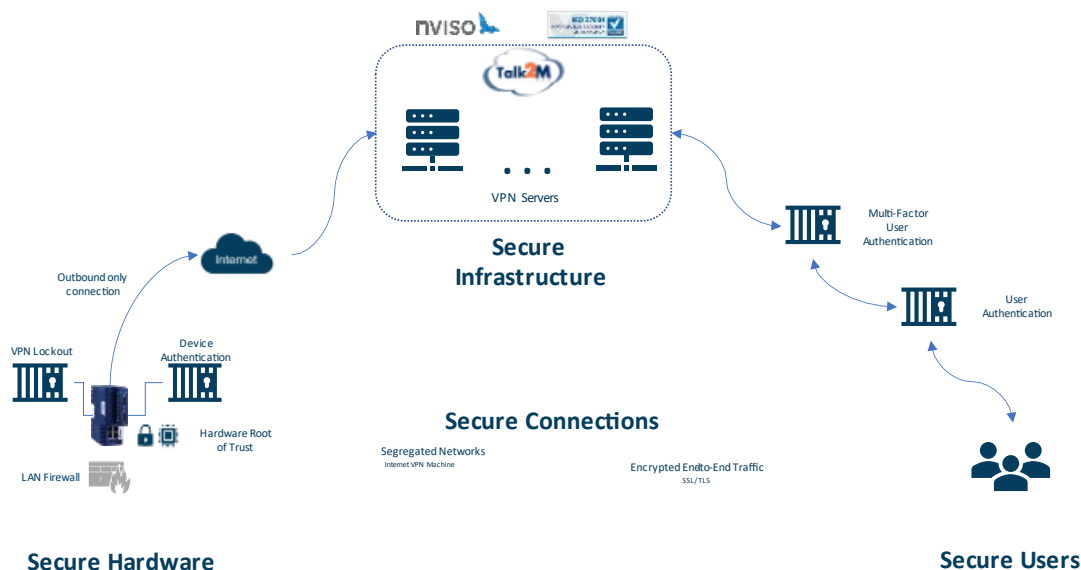
On the machine side, an industrial router is installed and connected to the core of the machine: a PLC (Programmable Logic Controller), an industrial PC, or any automated device – located inside a factory plant.

So, this architecture that would cover both the security and the ease of access for systems vendors would include the following:

- A dedicated VPN client router in the machine is to be accessed remotely.
- A cloud service such as VPN server connectivity provides additional security features such as filtering IPs or Ports, connection logs for audits, roles management, etc.
- A VPN client from which to connect securely to the machine

Compared to direct access to the machine, accessing the router through a secured cloud service provides an extra layer of security because only encrypted and authenticated traffic based on VPN will reach the router.

The following section lists a series of recommendations from the asset owner's point of view to be considered to allow any remote access to their machines.



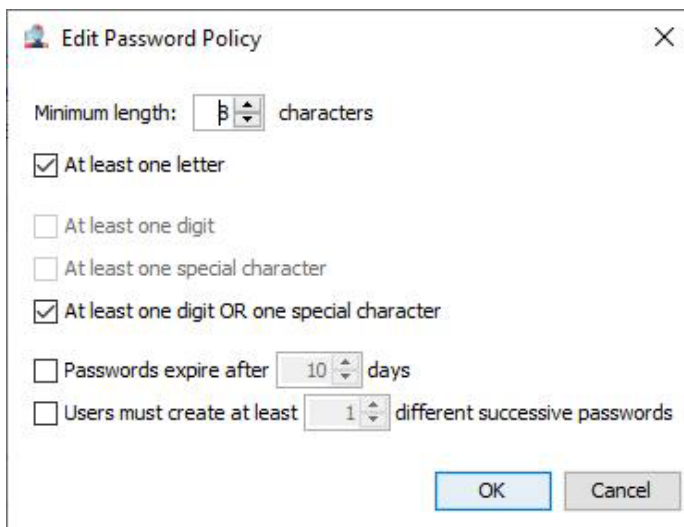
TOP RECOMMENDATIONS FOR SECURE REMOTE ACCESS TO INDUSTRIAL CONTROL SYSTEMS

4. RECOMMENDATIONS FOR A SECURE REMOTE ACCESS TO INDUSTRIAL CONTROL SYSTEMS

A) Identity

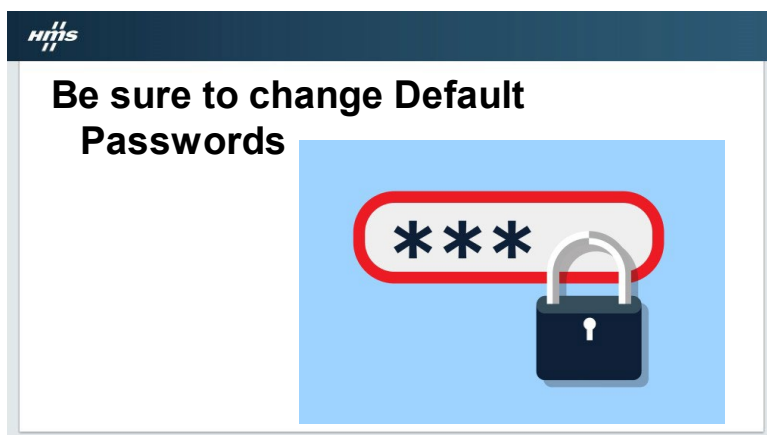
(1) *Apply recommended password policy in the PLC*

The goal of remote access is changing the machine's configuration by accessing the devices directly and controlling the machine, such as the PLC and HMI. A strong password policy in the PLC provides the ultimate layer of defense.



(2) *Change the default password when configuring the device for the first time*

Default passwords are well-known by the industrial automation community and can be easily found on the Internet or in any instructions manual. Don't forget to change the password of the device/application when configuring it for the first time. Changing the default passwords protects the system against unauthorized users using default passwords to gain access.



TOP RECOMMENDATIONS FOR SECURE REMOTE ACCESS TO INDUSTRIAL CONTROL SYSTEMS

(3) Use Multifactor authentication whenever possible

Multifactor authentication should be considered among the best practices in remote access to industrial machines as it provides an added layer of security. Passwords can be discovered or stolen (including by brute force attacks, in which possible passwords are tried until the password is found). Suppose the system requires a user to enter a second code of single use provided by an SMS sent to a mobile phone. In that case, the password itself becomes worthless (unless the user's cell phone has been stolen and has no protection code, the system administrator should change the credentials immediately).

However, in some emergency cases where a fast reaction is needed, using a second-factor authentication can become a "nuisance" for the engineer. Implementing the most appropriate solution for every situation is always recommended, as explained in (11).



B) User Management

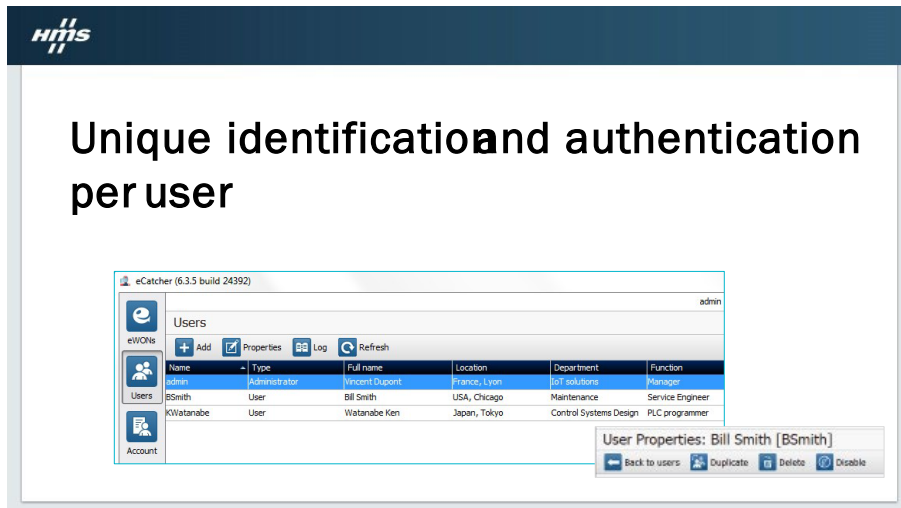
(4) Provide a unique identification and authentication per user

Every user must have a unique identification and authentication. In cases where a user's access needs to be revoked (for instance, an employee leaving the company), it should be possible to do so directly on the account.

Password policy and strength need to be configurable based on minimum length and variety of character types, a minimum lifetime, and forcing not to repeat used passwords. Only members of the Administrators group can edit the Password policy.

TOP RECOMMENDATIONS FOR SECURE REMOTE ACCESS TO INDUSTRIAL CONTROL SYSTEMS

Be sure to have systems obscuring feedback of the password entry to protect the information from possible exploitation by unauthorized individuals (i.e., displaying asterisks or other random characters when a human user inputs a password).



(5) *Define different rights per individual user*

A centralized management of the rights to access the machines at the server level offers an additional security-layer to user permission management. Every user must belong to a group that has assigned roles (permissions) to access routers or groups.

The system shall provide the capability to support unified account management. The system shall provide the capability to support the management of all accounts by authorized users, including adding, activating, modifying, disabling, and removing accounts. Members of the Administrators group must be able to temporarily block the access of a user having an existing profile and password without deleting it (during a planned leave, a job rotation, etc.).



TOP RECOMMENDATIONS FOR SECURE REMOTE ACCESS TO INDUSTRIAL CONTROL SYSTEMS

C) Damage Control

(6) *Only allow access when it is needed*

Vendors usually require remote access for emergency operational support and system maintenance. System maintenance is normally scheduled, and protocols for remote access connections can be established and monitored (for instance, linking the permission of access to a maintenance work order).

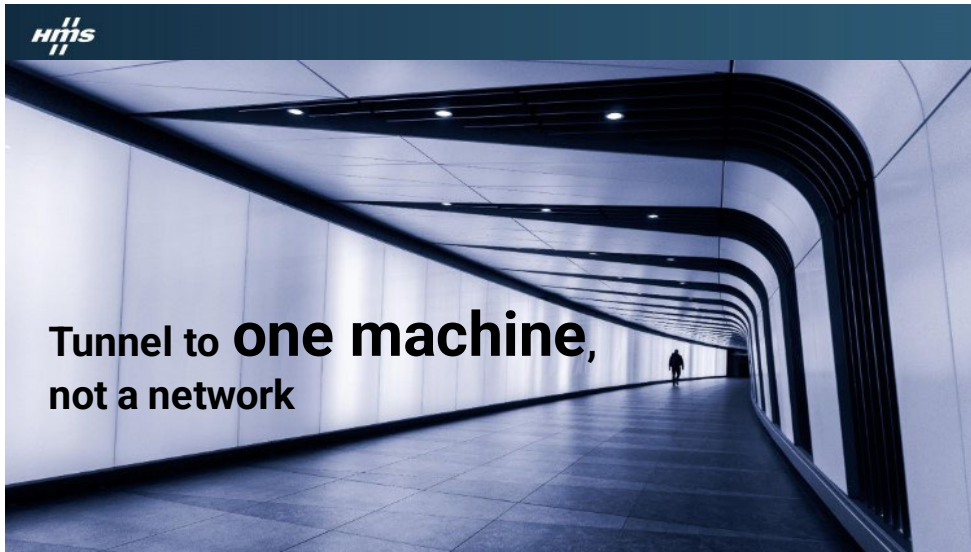
To provide additional security and control, the VPN or internet access might be enabled/disabled via a mechanical signal (a digital Input on the Router, which can be wired to a key-operated switch or a PLC output). The asset owner can disable vendor user remote connection until they are required to be enabled and disabled after completing their task. Moreover, all connection activity must be logged and ready to be audited. This allows discoveries of any unauthorized connections out of standard company procedures.



(7) *OEMs must have access to the machine, not to the Plant network*

OEMs should only reach the machines under their responsibility in the plant. To achieve this, the system must be configurable to segregate the machine network from the rest of the network. Once completed, the machine network nodes are not directly connected to the site network and must be configured with different IP addresses.

TOP RECOMMENDATIONS FOR SECURE REMOTE ACCESS TO INDUSTRIAL CONTROL SYSTEMS



(8) Avoid using one of the control devices in the machine (HMI, PC, PLC...) as a VPN host for the remote access

Using machine control equipment (such as a PC, HMI, or a PLC) as a VPN host may reduce its resources and degrade performance. To ensure the availability of the control system, it must provide the resources to operate in a degraded mode during a DoS event. An external router will act as a boundary to filter certain types of packets to protect control systems from being directly affected by DoS events, thus avoiding any external attack involving the control system and stopping the machine.

(9) Allow only outgoing connections from trusted to untrusted zones

No inbound firewall ports must be exposed on the Internet, and no static Internet IP addresses should be required.

The industrial router initiates an outbound secured VPN tunnel point-to-point with a specific account in the cloud. This tunnel is authenticated and encrypted with HTTPS and goes over the corporate network and through the firewall (outbound only). Once online, it travels to the cloud network along with remote access services.

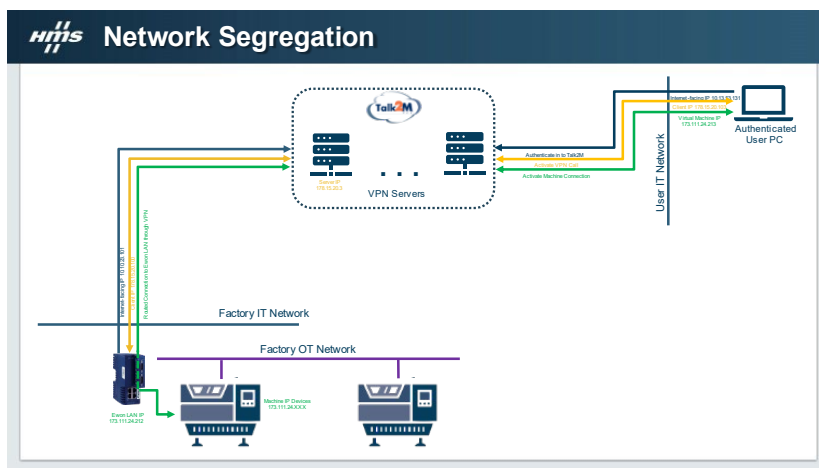
TOP RECOMMENDATIONS FOR SECURE REMOTE ACCESS TO INDUSTRIAL CONTROL SYSTEMS



(10) All Traffic must be encrypted

Remote support users connecting over the Internet should use a strongly encrypted protocol, such as running a VPN connection client, application server, or secure HTTP access, and authenticate using a strong mechanism, such as a token-based multi-factor authentication scheme.

For encryption, public Certifications from commonly accepted standards and guidelines must be used, such as the Internet Engineering Task Force (IETF) Request for Comment (RFC) 3647 for X.509-based PKI (Public Key Infrastructure of 2048 bits).

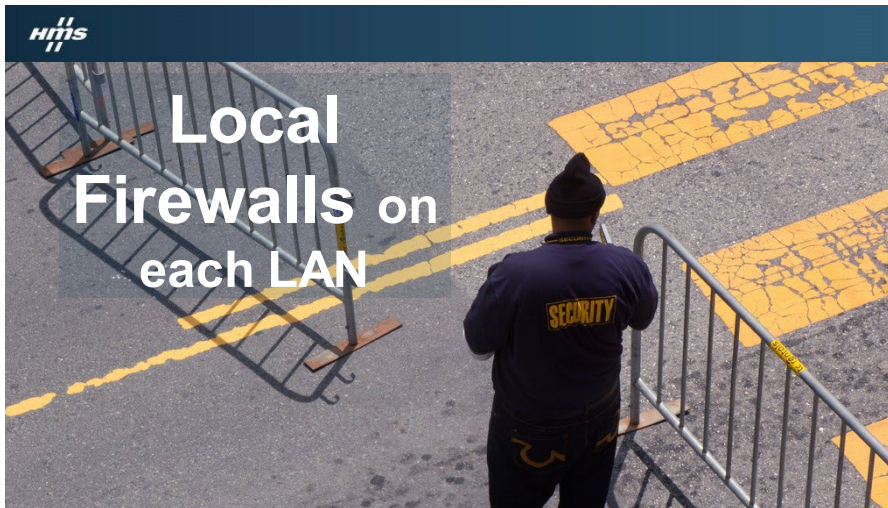


D) Limit Connectivity

TOP RECOMMENDATIONS FOR SECURE REMOTE ACCESS TO INDUSTRIAL CONTROL SYSTEMS

(11) Firewall and filter at a higher level

Access to the IP addresses and ports of the device should be restricted by configuration. This includes limiting a user's access to both Ethernet and gateway services. This filtering should happen outside the router itself.

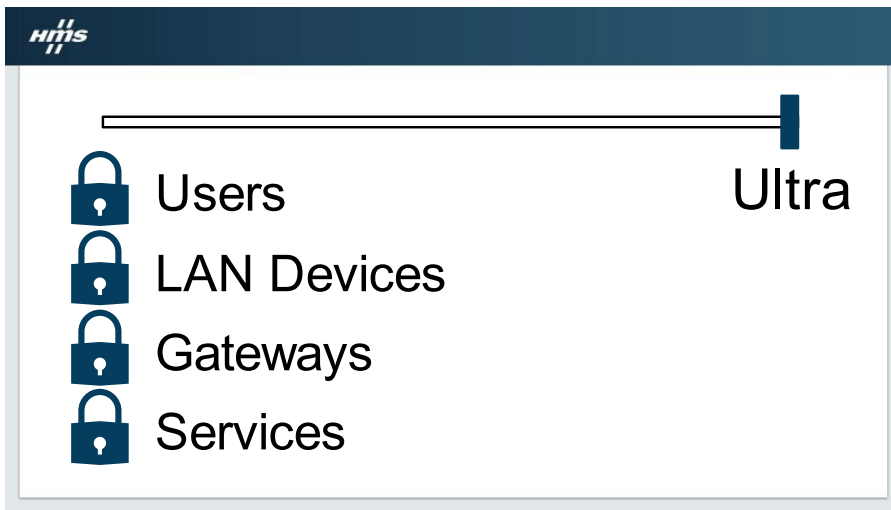


(12) The Router IP address must not be visible on the Internet

Router IP addresses must be hidden from the public to prevent hackers from scanning for potential targets easily. So, use only private VPN addresses to connect to the router instead of public IP addresses.

However, the router will still have a hidden IP address accessible through the Internet. Suppose the router is configured to have Internet access through a cellular modem. In that case, the WAN connection is equivalent to the cellular connection, thus putting the public IP address out on the Internet.

TOP RECOMMENDATIONS FOR SECURE REMOTE ACCESS TO INDUSTRIAL CONTROL SYSTEMS

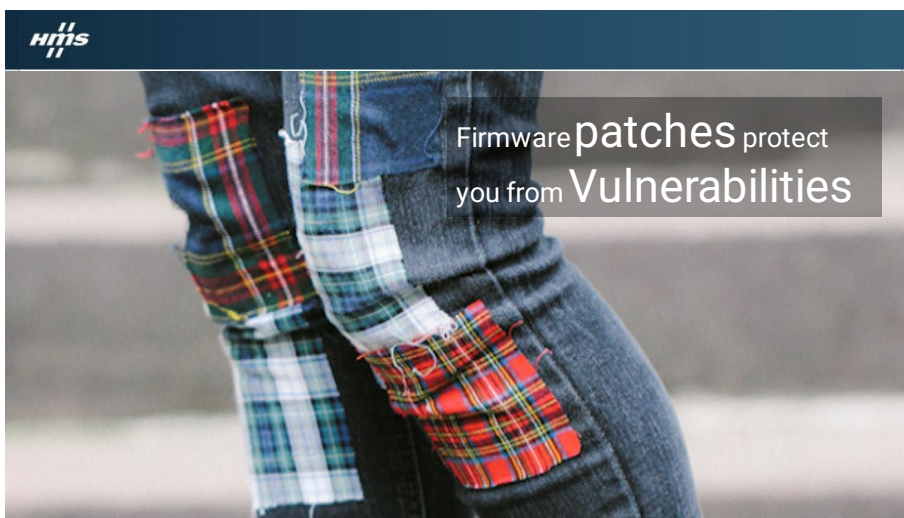


E) Update Your Defenses

(13) *Always update devices with the latest official firmware and apply security patches*

This is in accordance with the device manufacturer's recommendations. Moreover, you can be notified by the ICS-CERT (Industrial Control Systems Cyber Emergency) about vulnerabilities found in industrial automation equipment and receive recommendations for required patching as well.

Because the systems included in a remote access solution (router and cloud services) are not always critical and are often disconnected, it is not necessary to follow specific policies for the upgrade of the system other than those recommended by the manufacturer. For instance, the upgrade can be done at any moment the remote access is not being used, as it will not affect the availability of the machine in any case.



TOP RECOMMENDATIONS FOR SECURE REMOTE ACCESS TO INDUSTRIAL CONTROL SYSTEMS

(14) Be able to fully reset to factory settings

Your router must be ready to accept a reset to factory settings, including password, device Identification, User Web site, LAN IP address + mask, Internet access, Modem/WiFi settings, and cloud and Proxy access configuration. In cases where strange behavior is detected, the device must be fully restored to factory settings.

(15) Configure remote access according to your real needs: security vs. availability

Control systems and machines normally operate in real-time. Therefore, it is crucial to quickly connect to the systems when it is necessary to do so. Procedures or systems forced to perform the multiple steps required for remote access might drive operators to either (1) remove security features which slow down their connection process, or (2) create workarounds to allow fast connectivity. These practices, in addition to those that involve using the same password for every field device, reduce the chances of a secure remote access capability.

It is recommended to consider how to apply security procedures in cases where the highest priority is the availability of the machine, and remote access is crucial for that.

(16) The connections and changes must be auditable

The system must be capable of logging events on access control, errors, operating system, control system, backup and restore, configuration changes, potential reconnaissance activity, and audit log. Individual audit records shall include the timestamp, source (originating device, software process, or human user account), category, type, event ID, and event result.

(17) High Availability of the Remote Access service

Whenever remote access support is needed for emergency operational support, remote service becomes critical for the availability of the machine. Thus, the service provider of the access must guarantee high availability of the cloud service with an SLA (Service Level Agreement) reinforced by several actions and control objectives such as Monitoring and alarms management system for key performance indicators with on-duty 365/24/7 engineers.

[1] CPNI – Centre Protection National Infrastructure, *Configuring & managing remote access for industrial control systems*

[2] NIST – National Institute of Standards and Security, *Guide to Industrial Control Systems (ICS) Security*

[3] ISA - ISA-62443-3-3. *Security for industrial automation and control systems, System security requirements, and security levels*