vLOTO™ – A new Paradigm for Industrial Safe and Secure Remote Access

Abstract

Remote access to industrial control systems is no longer a nice-to-have, it is a must. The benefits of remote access are well-documented – reduced downtime and reduced support costs, both of which are directly proportional to profitable operations.

Remote access of industrial control systems can jeopardize the safety and security of machines and personnel if not properly implemented. This document concentrates on the safety part of remote access and how the ProSoft Connect™ secure remote access solution with virtual Lockout-Tagout, or vLOTO™, can solve this problem. Readers are encouraged to read another whitepaper, Security Considerations for Industrial Remote Access, which discusses security for remote access in detail.

Introduction

When a machine breaks down, remote access is crucial to reducing downtime. In a competitive world, the reduced time could well equate to keeping or losing a customer. The added benefit is reduced support costs. We know there is some hesitancy to implementing remote access because of security concerns.

But, there is also a second and equally important reason why remote faces some hesitation – safety, specifically machine safety. We all know why machine safety is important. The more pertinent questions is, how can machine safety be realized remotely so that customers can realize the full benefits of remote access? To answer this effectively, we have to first understand how machine safety is applied locally, today.

Local Machine Safety

The typical steps one may take before making machine changes locally is to:

- Ask permission from Supervisor & Operator
- Follow Lockout-Tagout procedure
- Check the set points
- Review HMI for status

Lockout-Tagout, or LOTO, is a well-documented safety procedure used by industry to ensure that machines cannot be energized accidentally. It ensures that only the person that placed the machine in LOTO position can unlock the machine from this state.

Now, let's look at how secure remote access works today.

How does Remote Access work today?

Remote access today is secure, especially when using industrial gateways built for this purpose. These gateways provide a secure connection to the machine zone, ensuring no access to the

enterprise zone. Once access to the gateway has been configured, the authorized user can remotely access the machine anytime, anywhere. This is advantageous as described earlier in this document. But, they have 24/7 unfettered access to the machines and can implement changes.
While this is very secure, it may not be very safe. Imagine a scenario in which a machine is running a process and an authorized person can securely access the machine, make changes not knowing the current state – consequences of such actions can be ruinous. Not just to the machine, but most importantly to the people working on the machines!

ProSoft Technology has solved this problem with vLOTO on the Connect platform. ProSoft Connect® is a cloud-native secure remote access solution with multiple layers of security including app-based 2F authentication, SSTP tunneling with unique credentials, 256-bit AES encryption, and an extensive audit trail of user activity and changes.

ProSoft now offers vLOTO™ Dynamic Authorization – a new paradigm for safe and secure remote access to your industrial control system.

What is vLOTO™ and how does it work?

vLOTO, or virtual Lockout-Tagout, enables the safe access that OT needs for reduced downtime and the secure control that IT requires. The feature allows authorized plant personnel to control when and how their industrial control systems are safely and securely accessed.

With vLOTO, authorized approvers hold the key. An authorized approver can be an IT Manager, plant engineer, machine operator, or a shift supervisor. Each authorized approver or a group of approvers:

- Must approve each secure remote access session
- Approve access for a specific amount of time
- Can deny or revoke access at any time

There is an extensive activity audit log of all user activity – permissions, acceptance, denials, and change of approver list. This audit log is un-editable and can be saved for future forensic use.

For the remote user, this means that they cannot access the machine at any time without prior approval. They must request access, specify the amount of access time required, and state a reason. Once they have received approval, they will be able to securely and safely access the industrial control system to perform the required changes. Once the session time expires, the remote user will automatically be locked out from accessing the control system. They will have to request permission and be approved again for safe and secure remote access. Since vLOTO allows for an approver to deny access at any time – if the conditions on the factory floor changes state, then an approver can revoke remote access instantly.

With vLOTO, a machine builder or system integrator can confidently propose remote access to their customers knowing that they will save time and money, not only for themselves but also for their customers. End customers can breathe easy after implementing remote access as they can control when someone can access their control system, remotely. Additionally, IT and OT can be fully involved in the process – OT gets the safe access it needs to keep downtime and maintenance to a minimum, while IT gets the control and data it needs to ensure the plant is secure!

Conclusion

Remote access is a must that will help reduce downtime and support costs, both of which are directly proportional to profitability. If remote access is not implemented correctly, it will jeopardize the safety and security of your industrial control system. ProSoft Connect with vLOTO is the only remote access solution that provides safe and secure remote access to your industrial control system. ProSoft Connect with vLOTO requires authorized users to request permission from an authorized approver prior to remotely connecting, safely and securely, to the industrial control system. The access can be denied or revoked at any time and an extensive log of user activity is maintained.