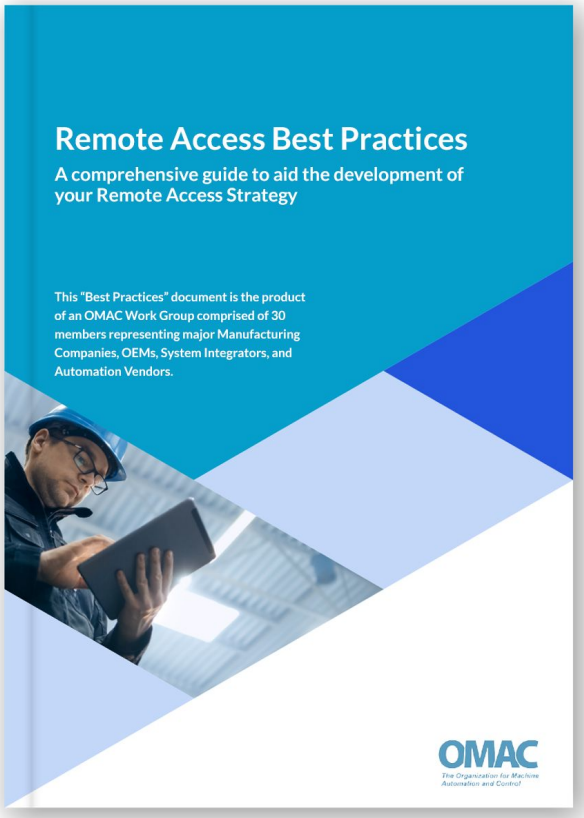
Session 6

Methodologies to Engage Beyond One-to-One



- 09 Sep - Kickoff Meeting
- 23 Sep - Current State and Stakeholders of Remote Access
- 07 Oct - Collaboration with IT
- 21 Oct - Classification of Remote Activities
- 04 Nov - Validation of Assets being Connected
- **18 Nov - Methodologies to Engage Beyond One-to-One**
- 02 Dec - Security and Safety, Documentation and Change Management
- 16 Dec - Review of Draft Report
- 13 Jan - Final Report Approval

Special Guest Speaker on Dec 02

Eric Byres, SCADA and ICS Security Product Visionary

One of the world's top experts in the field of SCADA security

Testified to the US Congress on the "Security of Industrial Control Systems in National Critical Infrastructures"

Recognized by various international organizations:

- IEEE Outstanding Industry Applications Article Prize in 2000
- 2004 "Donald P. Eckman Award"
- 2005 "Keith Otto Award" presented by the International Society of Automation (ISA).

Q1 - Should Remote Access to plant floor equipment to make changes be restricted and controlled by an assigned administrator?

- Having a single point of contact both helps simplify the workflow but enables better security
- It is imperative for safety and security that remote parties be channeled only to the appropriate equipment
- The owner of the system should be the administrator of any remote access
- Data changes should be controlled
- The plant manager would want to know that the remote access process is a controlled and coordinated activity
- Control and responsibility should be given to facility manager
- With a high-security level, an assigned administrator can have Remote Access
- Enforce communication of changes
- There should be a point of contact who can at least grant and remove remote access rights
- Change management needs to be considered
- Essential to have an approval/verification process that is logged and time-stamped
- Remote monitoring can be controlled by automated security, but the floor must approve the changes
- The group of people who can connect should be kept updated as well as their access to necessary equipment

Q2 - Should there be some centralized method to coordinate the Remote activities of various individuals?

- Best practice to control who can access what and not provide broad access to all systems. Having a centralized method to coordinate the access would make administering the access easier.
- There should be general central guidelines and policies in place that sites can utilize as a baseline
- The thought that every piece of equipment in a plant might have it's own remote access process and procedure is too complicated to consider seriously.
- Standard "management of change" should be in place
- At the very least there, should be a log of who accessed remotely, when, why, and what they did
- An overview, who has which remote access rights and a report about the last remote activities, is important. Here, you can have the control and manage all the remote activities.
- In complicated scenarios, perhaps some central real-time coordination is needed but only in special/complicated scenarios
- If multiple individuals connect, there should be something even as simple as a log identifying the last person to make changes, the changes that were made and the date they were made.
- Some control over remote activities needs to be coordinated. Having ad hoc access to systems without corresponding is dangerous for many reasons.
- A taskforce of plant engineer, factory operators familiar with the equipment. And coordinate with them
- Patterns for similar use cases that should cover 90% of the requests
- Essential to have an approval/verification process that is logged and time-stamped
- In some way, the multiple users need to be aware that the others are also working on the same machine
- A standard method is easier to work with than various ad-hoc workarounds

Q3 - If collaborating with multiple resources, should there be guidelines that all parties should follow?

- General safety guidelines aside - version control should be utilized and when coordinating multiple sources. Methodologies will vary based on technology being used, but individuals should be specific on the areas of code they are touching if nothing else.
- Guidelines would provide consistency. Resources should not be able to access any systems other than the ones they are responsible for.
- Someone needs to be in charge and coordinate the activity
- Management of Change process and procedures should be followed
- Coordination
- Policy guidelines including who will connect and how they will use the system.
- Changes need to be considered and access needs to be controlled to mitigate risk.
- Assign a task force that maintains the guidelines that consist of plant engineers, factory operators familiar with the machine.
- If I'm connecting as an OEM engineer, my access should reflect the ability to change/alter machinery. If I'm a customer using the same connection, I may be able to read only and not change functions. The guidelines really could be dependent on the type of connection as well
- All need to know the others are connected to the same machine
- Making sure that everyone is aware of what the others are doing. Ensuring that safety procedures are being followed.

Q4 - When given Remote Access, should it allow general access to all equipment or restricted to only specific devices?

- Ideally, users could be given access to only the equipment or devices they need access to. This requires a lot of effort though from a network management standpoint and may not be easily attained.
- General access should not be provided; resources should only access the systems for which they have responsibility.
- Remote Access should be restricted to specific devices and only when it is determined that there is a requirement to access other devices to correct an issue should access to those additional devices be allowed.
- Access rights should be only granted for the specific equipment and systems that support that system
- remote access to specific devices makes more sense.
- The more control you have over who accesses what, the safer. Not everyone should be trusted with complete access.
- Enforce the principle of least privilege
- Definitely, only specific devices that account/vendor is authorized for
- Restricted to controls devices that the user has permission to access
- Access to only the equipment required
- Only specific devices
- This depends on the situation. It may be beneficial to control access at the sub-device level due to job role and one's expertise.
- Only to devices that require the access for that moment in time
- Restricted to specific devices/machines rather than just a connection to the plant floor network.

Q5 - Should there be some method that validates the individual resource is the proper person?

- ALL resources accessing systems remotely should be uniquely identified
- This should be in the design protocol.
- Only people familiar with the approved and accepted policies and procedures should be allowed to participate in remote access activities. Would you want an unqualified person performing medical procedures on you?
- One must know who was in the system by individual not just group access
- Something like 2FA would go a long way in preventing malicious or unintended parties from gaining access
- A continuous validation procedure is essential. I think the "2-step verification" system from smartphones can be used.
- Ideally user account is created by IT, authenticated by the AD, account is within a special user-group, remote access platform has 2FA, and OT staff can specify the devices the account is whitelisted to access.
- Individual logins and audit trail would be ideal for tracking and tracing any issues and mitigating risk as per questions above.
- Two-factor authentication should be required.
- Two or three-tier authentication
- Requesting access, then an email or text to verify
- There should be some method but it may be on the supplier side The end user could potentially have a say in this as well,
- Authentication is required for security.

Q6 - Do you feel that there are risks in leaving a connection continually open for External Access?

- When a resource is done troubleshooting, they should close their connection. security standpoint, remote connections should not remain open.
- Access should be controlled - when granted, it should be only for the period for which it is applicable and then closed.
- Every remote access should be time-limited or extremely restricted in the type, quantity, and destinations of information accessible.
- If the access doors are closed and only opened when needed, it should stop accidental access to wrong areas
- Safety risk is high; the vulnerability of the system is increasing if you leave a connection continually.
- If proper security isn't in place it's like leaving the backdoor unlocked.
- No sustained, unused connections should remain in place. Connections should establish when needed - and be authenticated each time - and terminate when done.
- Yes this can open the network up for malicious intent.
- Intended or unintended access could harm people or equipment
- Leaving connections continually open presents the risk for accidental changes.
- Could be used for non approved use, could be spoofed
- Risks are always greater for cybersecurity if connections are available.

Q7 - Does the requirement to use the network infrastructure to reach a device create challenge?

- Technically there are challenges, but if designed properly, they can be overcome. In today's world, using the network is almost a necessity.
- The limitations of the infrastructure equipment and the capabilities of configuring the infrastructure equipment obviously restrict the type of access that can be granted.
- Almost 95% of all plants do not have a complete and accurate network make of all devices
- Having a converged industrial network is a big requirement for thorough remote access availability. However there are technologies available that can "circumvent" the plant network. These can/should be used with IT approval and only very high quality, secure technologies/platforms should be allowed.
- It doesn't have to if the network is set up properly (IT and OT segregation). But when not set up properly it can create challenges.
- If the manufacturing infrastructure is incapable of handling remote access, adequately implemented, black box type solutions can be viable.
- Not every device has Ethernet, not every device is connected to the network; if you have multiple segments, you need additional infrastructure to access the segments
- Really unknown - it depends on what you're dealing with as far as network infrastructure.
- We need to simplify the standard network infrastructure approach.

Q8 - When multiple users are working on the same problem, should only one user be allowed to make changes?

- We have safety protocols for accessing equipment in person, such as LOTO or captive keys. The same need exists for remote access
- The ultimate in remote access is NASA probes. We might want to see what they do with remote access when it comes to a few of these topics.
- Communication and detailed, up-to-date documentation is key to keep everyone on the same page and minimize (potentially harmful and/or outdated) assumptions about the current state of the configuration.
- Different people connecting often have different objectives and needs. Remote connectivity may not mean the same for everyone and I think a robust user access system is vital to asset and personnel safety.
- The key is communication between the multiple parties working collaboratively.
- There are Git-like solutions for machine code that would allow multiple contributors without overwriting code. These systems would need to be in place, and it would need to be clear before work began that it was segmentable.

Thank you for your participation

Looking forward to seeing you online in fourteen days.

OMAC
The Organization for Machine Automation and Control

ei 3