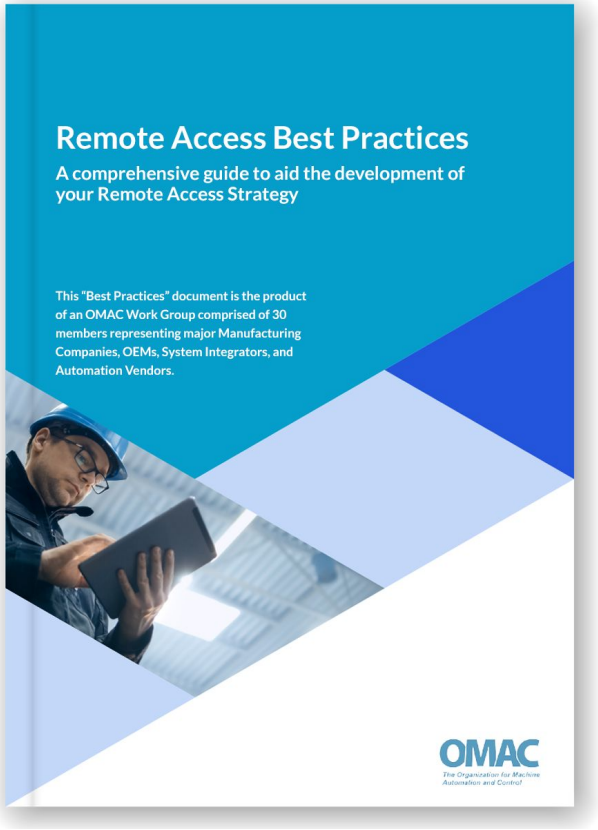
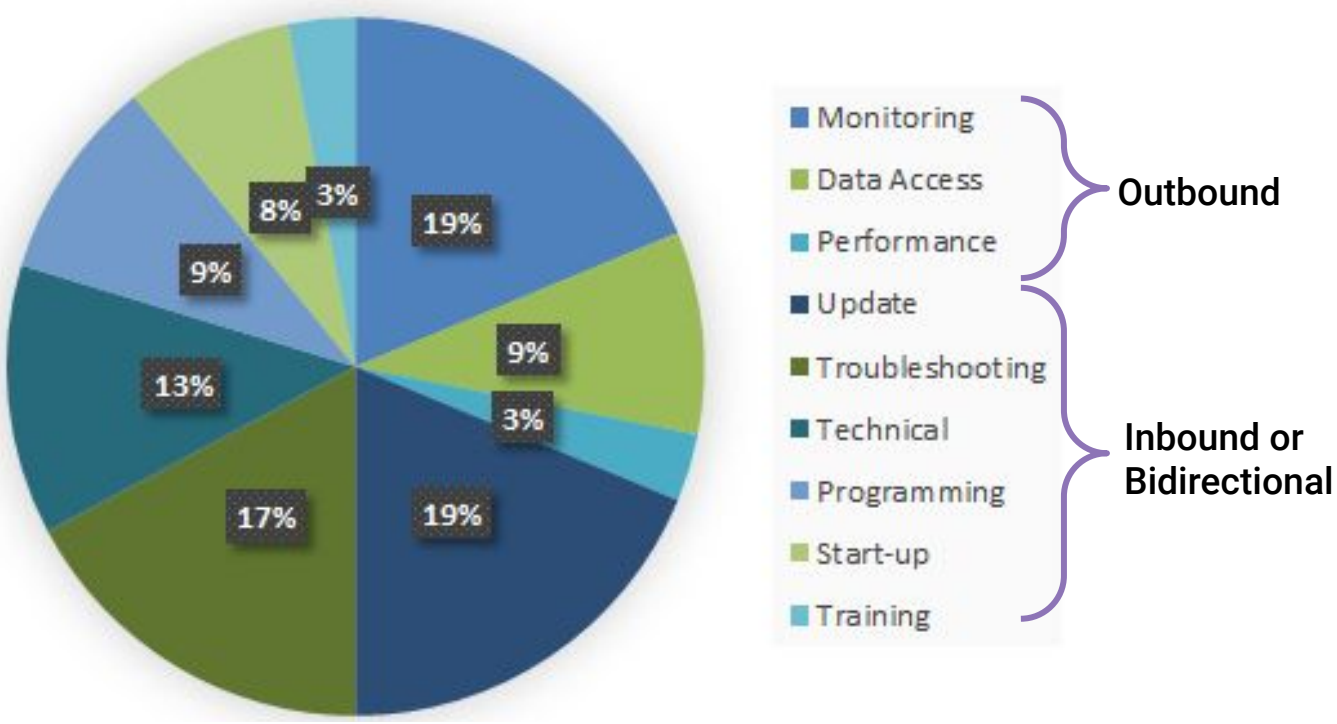
Session 4

Classification of Remote Activities



- 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

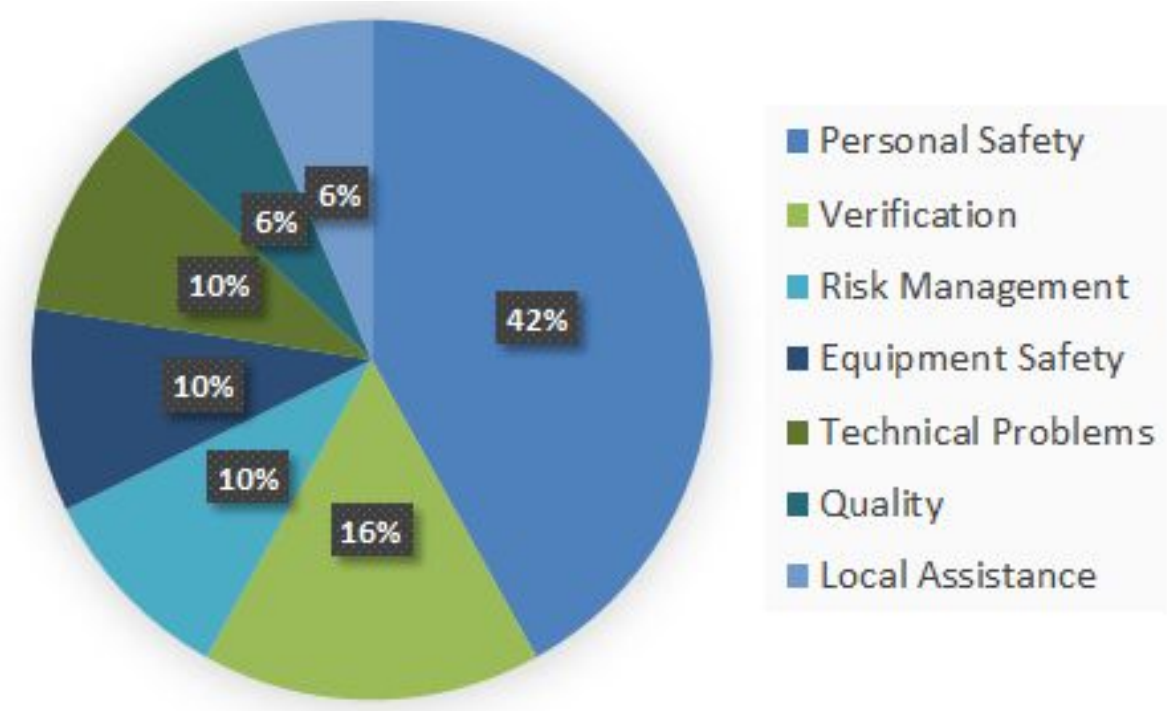
Q1 - What activities can be performed remotely?



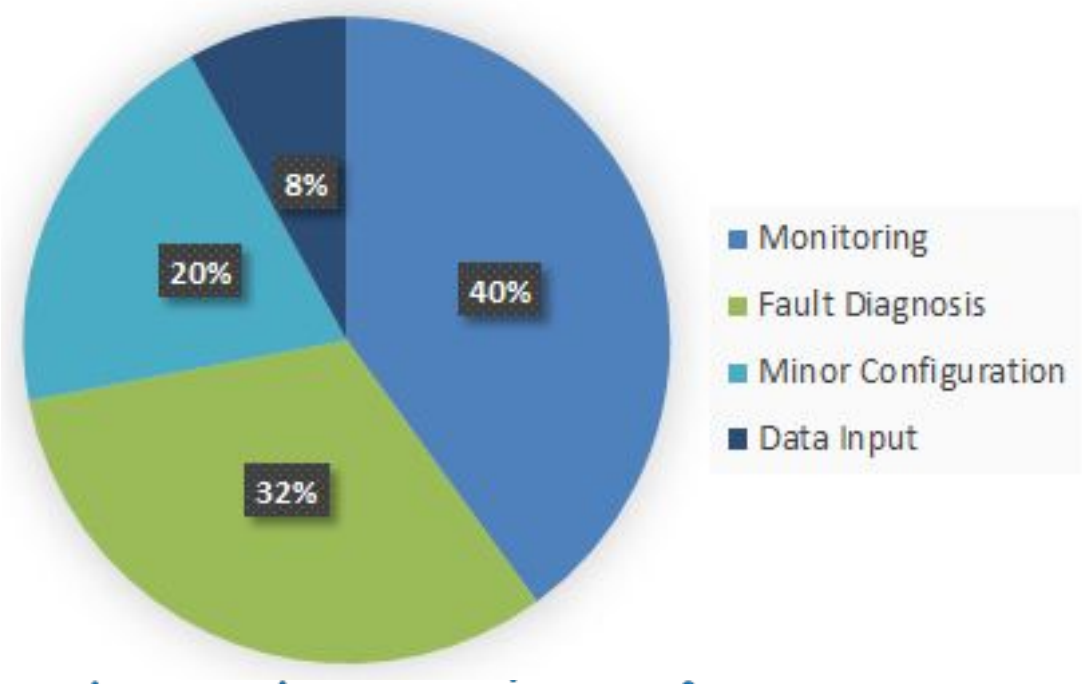
Q2 - Are there some remote activities that require someone to be present at the machine site (escorted access)?

- All changes require someone to be at the machine to observe/prevent access while changes are being made and ensure there are no adverse effects to quality.
- Any activity that could possibly alter a program should require on-site presence while and when remote access is granted.
- Modification or "soft jumpers" Forcing a PLC output or loading new software or updates.
- Any motion or safety changes. May also include any functional changes that affect the expected sequence of operation.
- Equipment that can cause bodily harm requires an onsite escort to verify people are clear of moving parts.
- If downloads are required, we send someone over to the PLC to place the key in Remote mode.
- Code changes Software Installation Patches / Updates Rebooting computers Any activity where safety is an issue.
- Commissioning (Supported by instrument guy in the plant)
- Troubleshoot IO
- Anything that involves a change being made to the control, updates or anything that alters the functionality of the equipment in any way.
- Updating Controls Systems should always be done with an escort. Anytime your actions remotely could have a physical response, there needs to be an escort.
- For safety, any PLC changes we require someone to be on site via voice to verify any activity at site.
- Some commissioning activities. Patching & backup activities. Verification for troubleshooting resolution. Verification after reboots.
- Program downloading Program modification
- Changes that involve shutting down the machine, that disrupt the network or potentially impact safety.
- For us, all activities require someone nearby. We didn't build the machine; we're there as backup/troubleshooting. Anything that can making anything move, turn on, heat up or make a machine dangerous needs someone by the machine. Any command to make a motion should be started locally. Cordoning off specific machines in ways that prevent entry to allow remote start may not require someone present. "This machine is remotely controlled and may start unexpectedly."

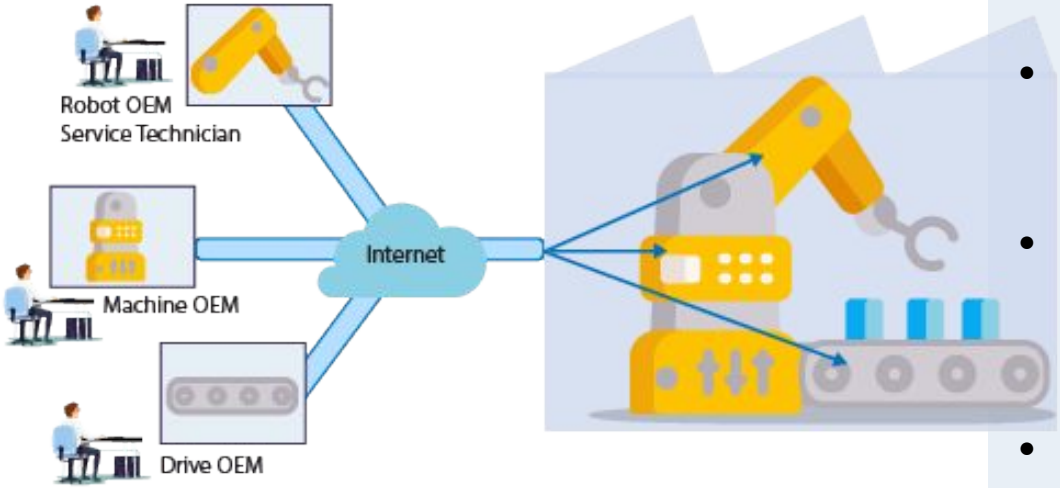
Q3 - What are some reasons that require escorted access?



Q4 - Which activities can be performed without the need of escorted access?



Q5 - Are there activities that could require collaborative remote access?



- **Frequently have multiple people online with the same piece of equipment at a time** - either troubleshooting the same issues or different issues.
- If a machine has several **components from different suppliers and the issue is not clear**, then you need a collaborative remote access.
- **Auditing connected process** affects and status. If there are connected process on the **input or output side of the equipment being connected to there needs to be input on what else is going on.**
- In many cases troubleshooting requires collaboration between someone on site who can identify something physically wrong and an engineer working remotely to point them in the right direction. **We will occasionally pull in a manufacturer rep if things get really strange**.
- As an **automation vendor, everything we do remotely is collaborative**, if it's gotten to the point we need to be involved we want the **machine builder who wrote the code to be with us so we can teach what it is we are doing to increase the independence of the machine builder/end user**. Any command to make the machine go should be issued locally by someone who can see and verify it is OK to do so.

Q6 - Are there access rules which relate to machine states (eg. if the machine is in production..)?

- I can't think of any rules that apply to local access to equipment that shouldn't also apply to remote equipment access.
- **Safety rules should apply** to hazardous chemical areas sensors and protection equipment. Rules apply to Burner management systems many times written into the software of programing
- **Currently a manual process that is based on a mutual agreement** that the 3rd party does not access without approval.
- **A machine in production should only allow for read/view access.** Offline or backup machines can be controlled remotely provided there are no safety concerns
- Yes. **There must be something like a traffic signal**, where the access rules are clearly defined.
- If the machine is in production you shouldn't be able to get online with the PLC without an escort
- **We don't have specific rules but if we're involved it’s because the machine is not producing.**
- **Not really because once you have access you can change the machine state.**

Q7 - Are any of these protocols tied to any Environmental Health and Safety (EH&S) policies or other policies?

- Safety systems primary but also environmental systems like stack gases on Boilers
- In most cases, safety is the driving factor. **Changes to a running machine can have fatal consequences**.
- **As an OEM, we do not have any**. We do **have customers that have EH&S policies that dictate this connection**. We have seen customers remove the connection to our equipment completely and have to request connections through their designated channels.
- We consider it an **EHS issue on our side** and many of our customers do as well.
- **In the EU the Machinery Directive EN60204 defines a lot of what has to be done to start a machine including what is required for automatic/remote functionality.** This was a challenge for one customer trying to do full line automatic production/changeover. Everything all machines ready to go with proper recipes loaded, and then **someone has to run down the row of machines and hit start on all of them.** (that may have been a customers interpretation of the machinery directive and/or be an old standard)

Q8 - Do you, or should you consider the liability impact of Remote Access?

Special Guest Speaker

Mark Voigtmann, Partner at Faegre Drinker

Leader of automation practice at Top 50 law firm

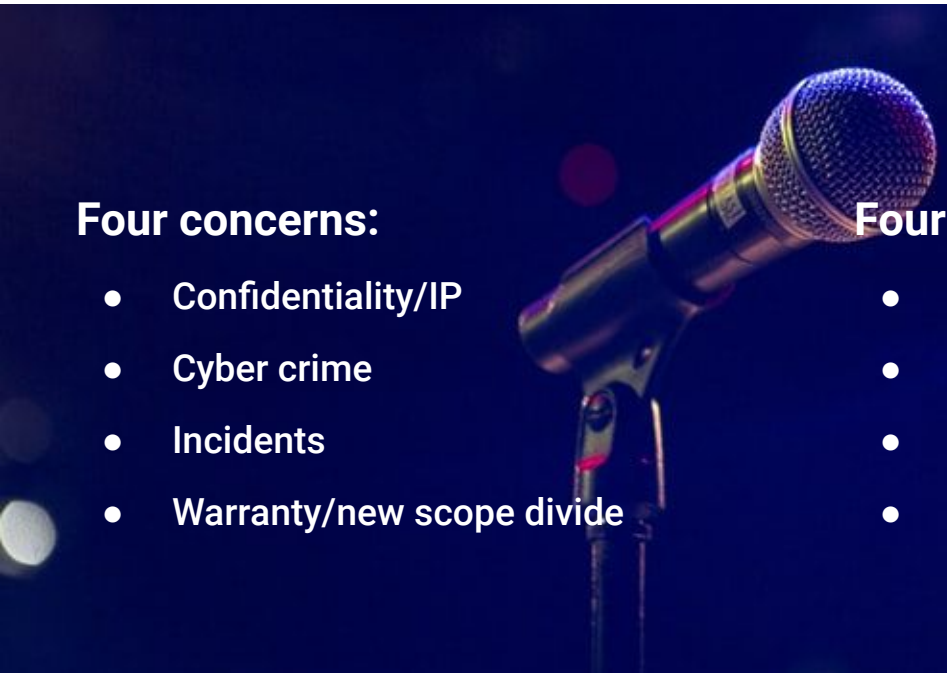
Author of the Automation Legal Reference (ISA 2013)

Mark.Voigtmann@faegredrinker.com

Q8 - Do you, or should you consider the liability impact of Remote Access?

Special Guest Speaker

Mark Voigtmann, Partner at Faegre Drinker



Four concerns:

- Confidentiality/IP
- Cyber crime
- Incidents
- Warranty/new scope divide

Four legal tools:

- Thoughtful, two-sided clauses (addressing each concern)
- Indemnity
- Incorporation of “standard”
- Waiver of consequential damages

Next Questionnaire: Validation of Assets being Connected

1. What devices do you expect require connection for remote support?
2. Are there any devices that you do not think should or would not be connected?
3. How do you connect to these devices in the plant?
   a. Serial Port (RS232/485)
   b. Fieldbus connection
   c. Ethernet Connection
   d. Through an intermediate Computer
   e. Other _____
4. If not directly connected to the device, how do you determine if you are connected to the correct device?
5. What actions are required to validate that one or more devices are accurate?
6. Is it important to be able to have connection to several devices at one time for doing troubleshooting? Yes or No. If yes please explain _____
7. Do you know of occurrences of connecting to the wrong device? Yes or No. If yes please explain.
8. What suggestions or recommendations do you have for ensuring the right devices are selected?

Thank you for your participation

Looking forward to seeing you online in fourteen days.

OMAC
The Organization for Machine Automation and Control

ei 3