Welcome to Session 3 on “Collaboration with IT”

AGENDA

#1 Questionnaire Response Review – Collaboration with IT

Each Topic from the Members Questionnaire will be reviewed and discussed by the members. Input will be solicited to gain feedback from the group with the intent to use this to create a “Best Practices” document.

Next Work Group Questionnaire – Classification of Activities

We plan to send out the next focused questionnaire on Oct 12. We request that members submit questions that will help provide substance to the topic bythen.

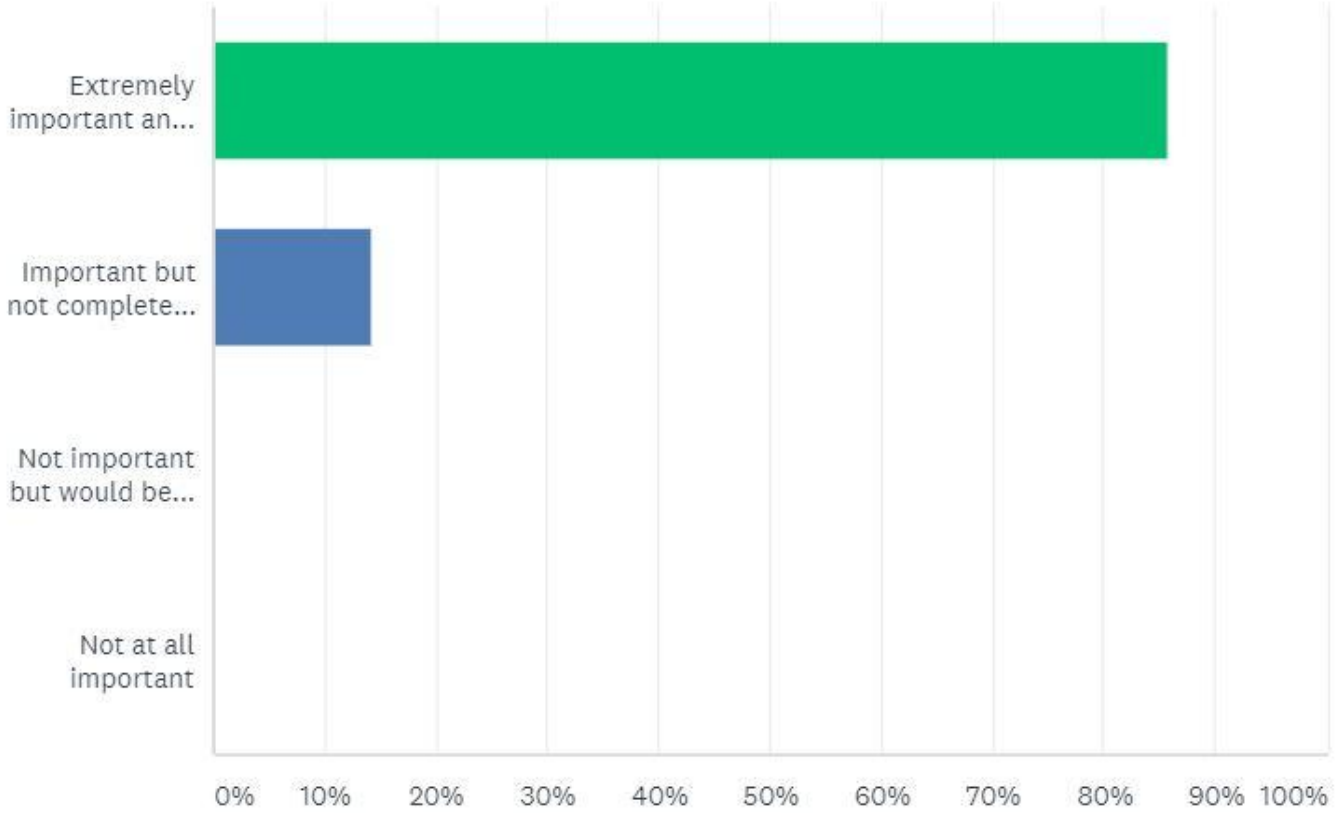
Optional Time for members to interact

Members can continue to be online for the opportunity to interact with each other. There is no planned topics for this time and this will not be included in the meeting recording.

Mark Fondl
V.P. of Product Management - Remote Access

07 Oct 2020

Q1 - Please indicate the importance of establishing a cooperative IT/OT working relationship:



Q2 - What activities can contribute to a positive outcome in your IT/OT interactions?

- Gain an understanding of each other's roles
- Agree upon objectives
- Continual communication
- Regular meetings to exchange knowledge about new technology
- OT to better prepare for discussion with IT
- OT takes the lead (?)

Q3 - What activities have created problems in an IT/OT relationship that should be avoided?

- Bypassing IT
- Ignoring each other; creating isolation between the two organizations; lack of communication
- Lack of a well defined or easily accessible approval process
- Not knowing each other's language, priorities and concerns
- Autocratic structure
- One side takes action that affects the other side without proper approval
- No clearly defined decision makers on either sides

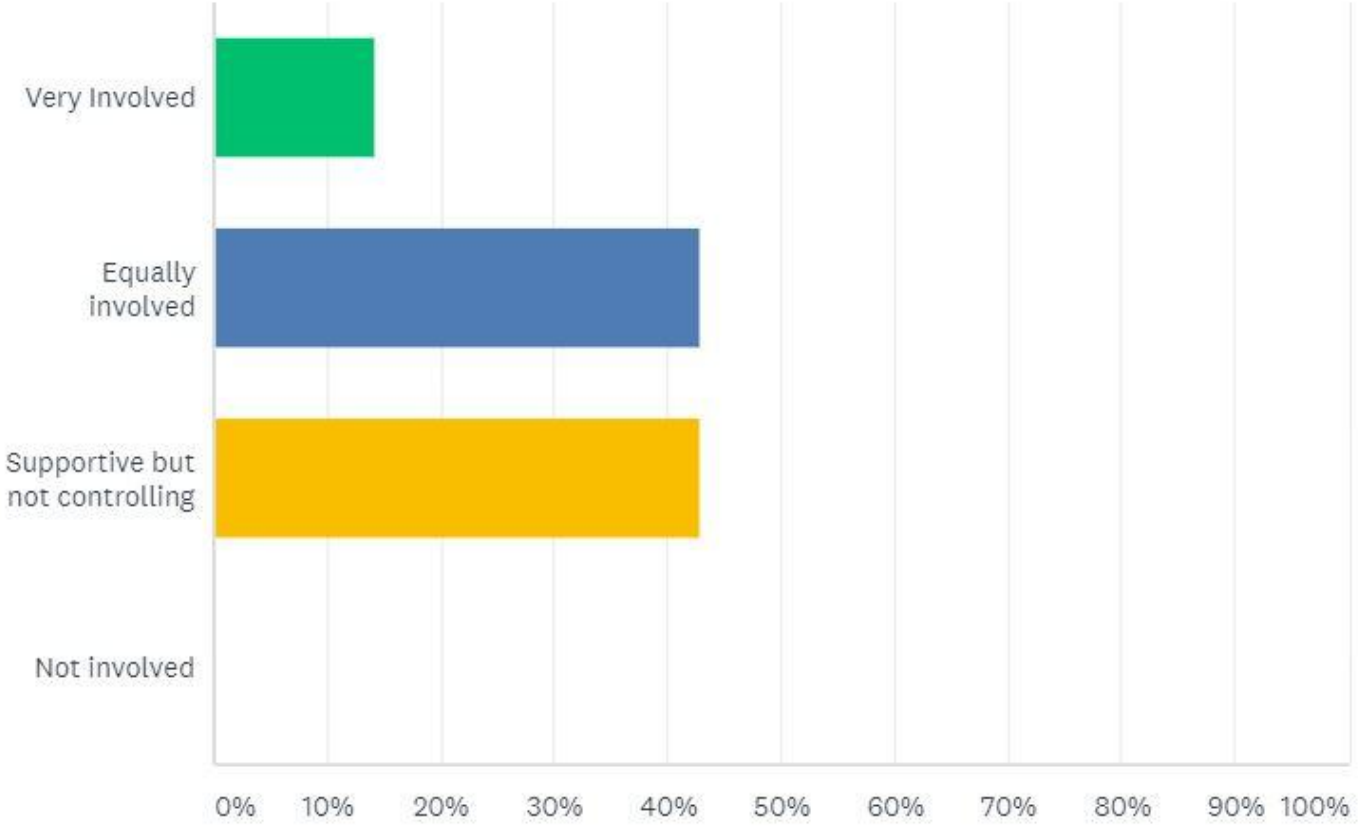
Q4 - What different priorities with IT and OT organizations can cause issues? How can these be addressed?

- CIA versus AIC concept:
  Confidentiality is a priority for IT versus Accessibility is more important for OT
- IT prioritizes the ability to dynamically make / push down updates. OT prioritizes stability (static systems) and the ability to thoroughly test updates before they are implemented.
- IT Organizations tend to have an established protocol for change management. From an OT perspective it can be seen as a lot of "Red Tape" and make it difficult to get things done in the time frame that OT is used to.
- OT wants to use what's tested and proven and IT wants to use the latest and greatest

Q5 - What are some of the key initial steps to create a better IT/OT working relationship?

- Shared purpose with agreed upon priority
- Communicate, Communicate, Communicate
- Creating "user requirements" that IT can take to develop a solution that meets the need
- Transparency in IT/OT efforts; creating an understanding what the other "side" does
- Accountability on both sides
- A well documented network architecture/blueprint and standards in place for the OT network so that both groups can speak the same language
- Leveraging reference documents

Q6 - How involved should IT be with the ability to access equipment on the manufacturing networks?



Q7 - What are the challenges as an outside company when dealing with a customer's IT group? If you are an end-user, do you have recommendations for outside companies to deal with your IT team?

- Work with both IT and OT to align your solution with their requirements
- Best to have a proxy at the OT act as the "customer" to IT
- Connect with the right IT professionals who both understand your needs and who have the time and ability to help.
- Have a single-point of contact (usually tied to the work being done) who can advocate on behalf of the outside company and escalate appropriately as it relates to the work that needs to be done.
- IT / OT should have a set of standards for outside groups attempting to access the systems
- Expect long decision process and have patience. Reference material and a proven track record may expedite the decision process.

Q8 - Can an outside vendor get permission to use another method for remote access? If yes, can you indicate what is usually required?

- If the vendor can show and ensure the security level of the alternative method, then he can get the permission.
- You need to work with an interested party high enough in the management chain with the kind of clout to get that permission
- This depends heavily on the end user company. Some companies are more flexible and others are extremely rigid.
- During an emergency at a plant site, sometimes Network access rules are overridden when Safety systems or major production and quality systems have failures
- IT approval required in collaboration with OT. Ensure that the solution is vetted and mutually agreed.

Q9 - It would be interesting to get your thoughts on the below statement, about whether this will remain or evolve?

“There's a large segment of facilities and industries that do not have dedicated IT people and the machine network is not managed or designed to deal with security issues, let alone remote access. We find that most of the time, these end users are in unregulated industries (unlike Food & Bev, Pharma, Automotive) and therefore have not needed to have the Enterprise side of the network gathering data or monitoring machine performance, where IT departments would typically get involved.”

- This will evolve because data is becoming the most important asset in all industries.
- This is a very realistic scenario, it should get a bit more secure by design.
- There will always be new organizations starting, and growing, which will grow through this phase of maturity.
- I have definitely witnessed this in a large percentage of our customer base. I've seen one customer who recently was attacked and changed their mind set very quickly about the viability of this approach
- Handling Break/Fix issues with plants is the most expensive method of maintenance

10 - If there's no IT department managing plant floor networks, who is usually in charge of the plant network?

- Maintenance
- There are also small teams within the OT department, who are in charge of the plant network.
- The plant manager.
- Whoever wants the connection. We have customers that are using a router provided by their ISP and no network security in place.
- The integrator, contractor, vendor or a local unofficial OT expert
- Nobody. In our customers, I see either IT managing it, or nobody. When OT manages it, they're minimally managing it.
- If everyone does their own thing bad things can happen.

11 - If you're an OEM, is this usually better or worse than dealing with an IT department?

- Better. Only because we feel comfortable about the security of our connection. If we didn't have a proven solution, I would feel worse about connecting these machines onto an unsecure network.
- It very much depends on the customer. In some cases IT is helpful and understands what we need; in others they just say no to everything. The same is true with the largely unmanaged networks with no IT support.
- We usually have a much clearer runway in these situations, there is a lot less red tape to cut through. But our goal is not to get our stuff working at the expense of our customers, but to help the customers put the most robust and secure means in place possible.

Next Questionnaire: Classification of Activities

- What activities can be performed remotely? Please list them.
- Do you have particular protocols in place to govern remote access of equipment?
- Are any of these protocols tied to any Environmental Health and Safety (EH&S) policies or other policies?
- Are there some Remote Activities that require someone to be present at the machine site (escorted access)?
- Why is the escorted access required?
- Are there activities that require collaborative remote access? Please list them.
- Are there access rules which relate to machine states (eg. if the machine is in production..)?
- Do you have methods to log access and the activities that were done during the remote session.

Thank you for your participation

Looking forward to seeing you online in fourteen days.

OMAC
The Organization for Machine Automation and Control

ei 3