Reviewing the

Current State and Stakeholders of Remote Access

Mark Fondl

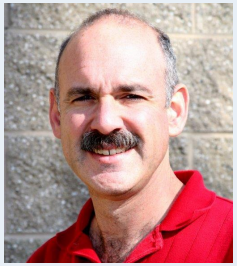
V.P. of Product Management - Remote Access

23 Sep 2020

Before we get started

- Please welcome the four new members:

Gerald Norz
Vice President Aftermarket Service at Durr



Larry Saidman
Chief Technologist - R&D at Nordson

Justin Jeanes
Digital Leader at ITW Hartness

Dr. Mehmet Sanlialp
Vertical Industry Manager at Mitsubishi Electric Europe B.V.

- Recap of the last meeting: Role of the Workgroup Leader and the Members
- Use the “Raise Hand” button to participate in the discussions.
- This meeting is being recorded. An archive of the event will be sent on Sep 30.

Agenda

General Questionnaire to be released

The General Questionnaire covering a wide area of topics will be sent out to other end users, OEMs, SIs and automation vendors outside the workgroup to obtain a greater number of responses. The results will be available to all members and used when reviewing the topic areas that we will be discussing in the future meetings.

#1 Questionnaire Response Review – Current State and Stakeholders of Remote Access

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.

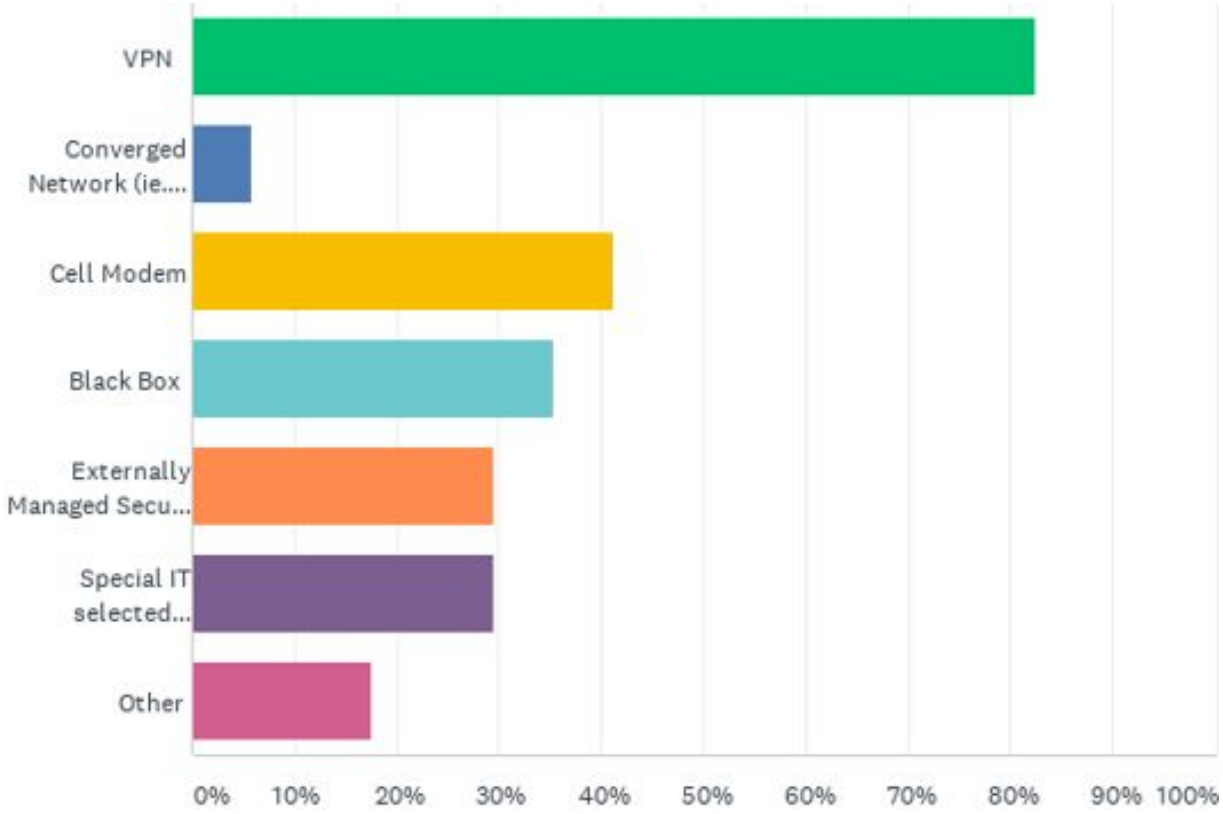
Next Work Group Questionnaire – IT Collaboration

We plan to send out the next focused questionnaire on Sep 30. We request that members submit questions that will help provide substance to the topic bythen.

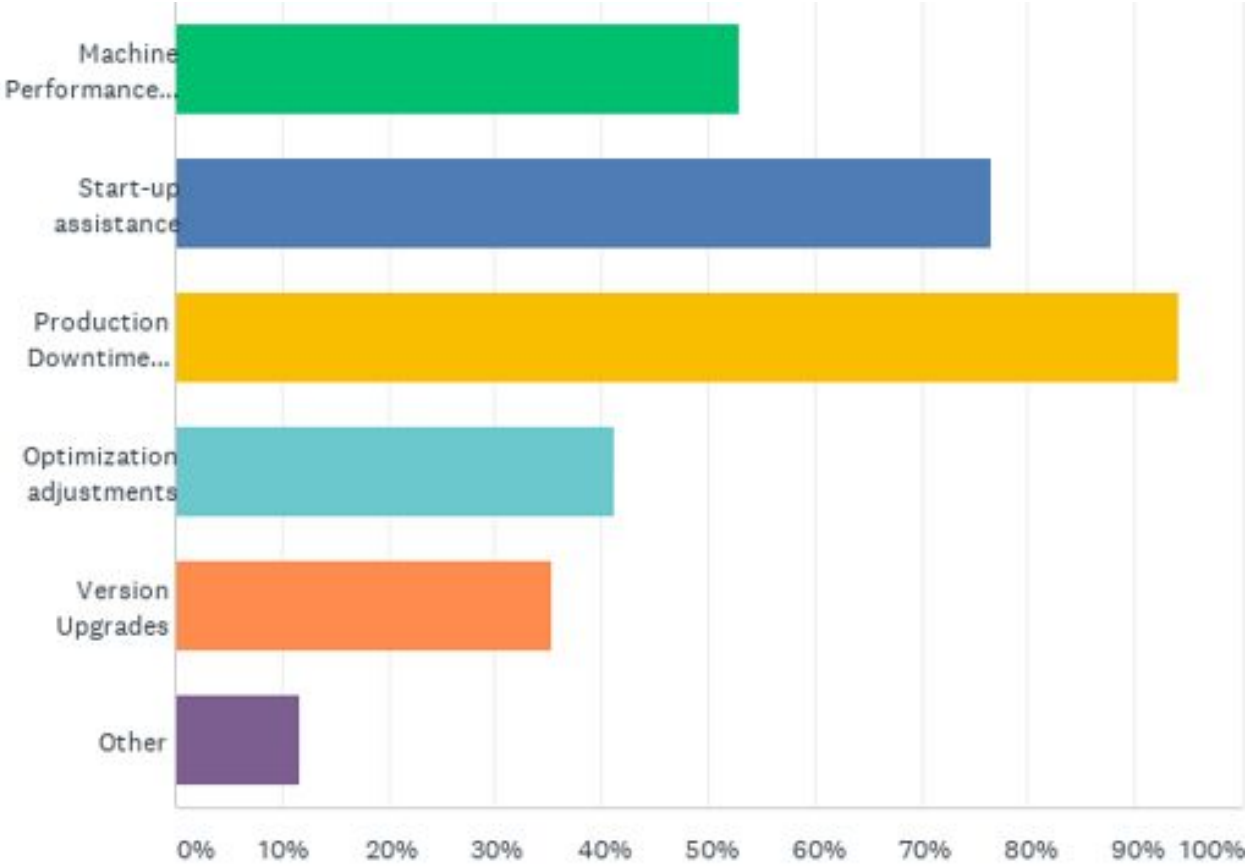
Optional Time for members to interact

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 recorded.

Q1 - Which methods of Remote Access are currently being used?



Q2 - What is the primary reason for using Remote Access?



Q3 - What steps do you recommend for doing a current assessment of Remote Access to determine the current use and coverage area?

- **Asset inventory to identify assets** that are self supported or 3rd party supported.
  - Determine from the **asset inventory which are internally accessible** through network resources.
  - For those **assets not currently connected** but require remote access for support, identify technical requirements to get them connected internally.

- Contacting our corporate information security department to **run a report on VPN usage per manufacturing facility**

- **Driven by domain experts:** What use cases does the remote access serve? Driven by OT experts: What facilities are used remotely? Which interfaces? Driven by IT: How are the facilities connected to the remote access solution? Which technologies are used? Which security precautions have been taken?

- **OT Network scan for known/unknown devices**

- **Analysis of number of non-employee remote access users setup in system,** analysis of employee remote access utilization, breakdown of different systems that remote access is being used for

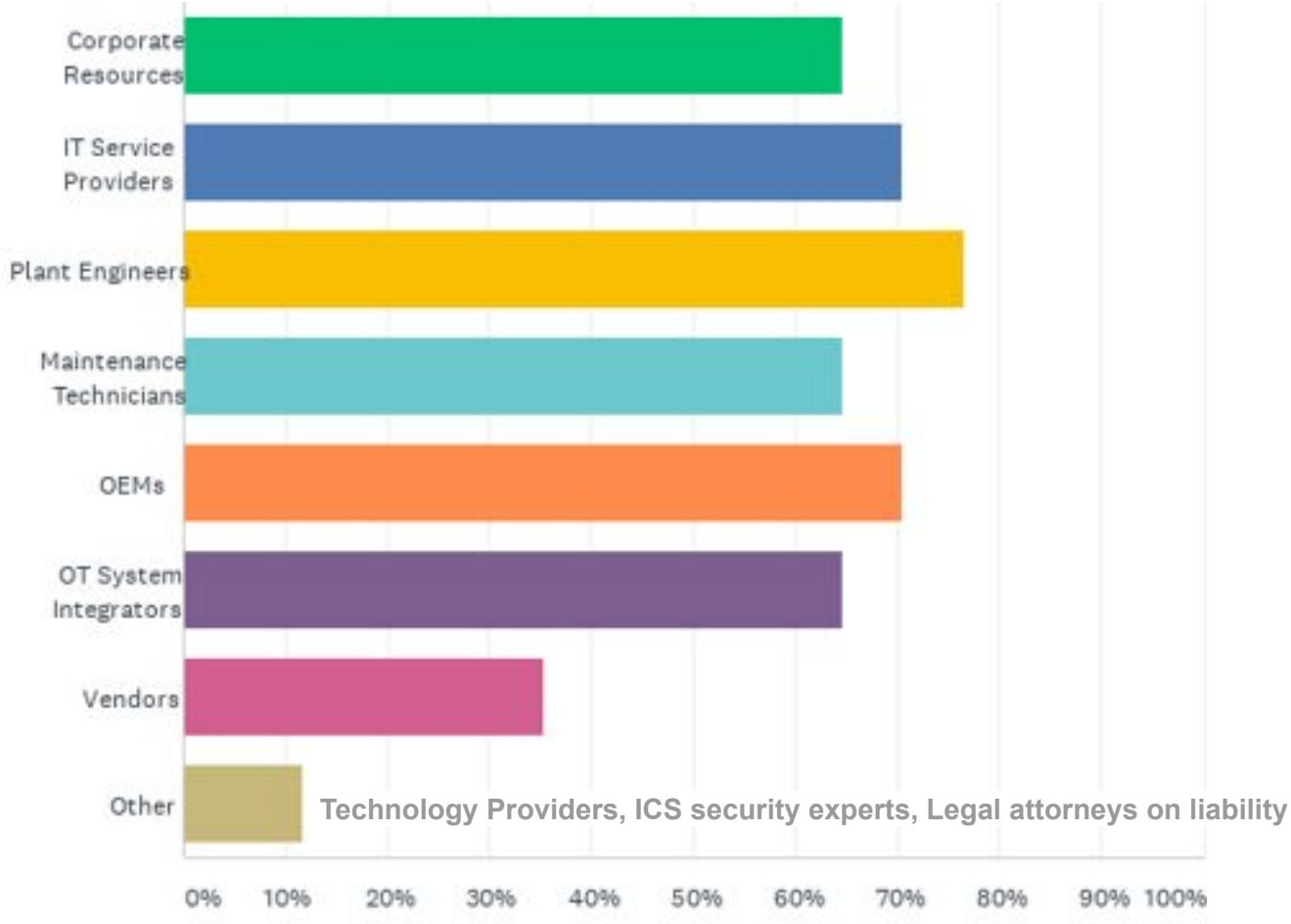
Q3 - What steps do you recommend for doing a current assessment of Remote Access to determine the current use and coverage area?

- In our experience, many customers **let multiple vendors into their plant network for remote access,** it's not usually limited to just one. Surveying OEMs and other service providers would be next in my opinion as they could paint a picture of regions and use cases.

- **Determine what methods / tools are utilized**. **Discuss ease of use of the tools. Evaluate the security** of the methods is use. Collect use cases. Why is Remote Access required. Who determines if access is granted.

- **Collect information from all third parties** on what their capabilities (both current and desired) are for remote support. Determine what infrastructure is in place already (firewalls, DMZ, cellular signal, network segmentation, etc). Determine who all the stakeholders are, which third parties need access, and who is a good contact for setting that up with each party, what type of connection do each of them need and what do they plan to do with it?

Q4 - What individuals are/should be involved with Remote Access



Technology Providers, ICS security experts, Legal attorneys on liability

Q5 - What training materials or guidelines do you currently have with regards to using Remote Access?

- **None really - largely done on an ad-hoc basis.** In most cases we're dealing with either **machine startups or breakdowns and IT is unavailable or unwilling to assist** so we work through remote access on a technician's laptop either through plant wifi or cell hotspot.
- We have a **white paper and a spec sheet that we developed to give to our customers** to explain our preferred method.
- **None**
- We remote into our customers systems via their remote access setups. **Documentation is not commonly available.** Sometimes IT issues automated emails with some instruction which needs to be worked through to set up and debug with a little bit of patience and help from IT.
- **Nil. Internal informal training**.
- Internal guidelines on VPN, Firewall and access control. **Not much formal documentation**.
- There is a required **corporate training - geared more towards what not to do rather than what to do**. Generally points employees to IT. There are standards and documentation that exist but very hard to penetrate and ultimately need someone from IT to act on it.
- Our **internal security department has white pages for guiding persons through setup and configuration of PC**

Q6 - What Glossary of Terms do you recommend we include with the Best Practices document?

- Overview and definition of each layer in the Purdue Model. Use to aid in defining technical access requirements in the level 0, 1/cell level network.
- ICS - Industrial Control Systems WAN LAN End-to-End Encryption Whitelisting Security Operations Center MFA/2FA Access Control Hardening / No Inbound Ports Defense in Depth Zero Trust LDAP & AD Active Directory User Groups Security Logs
- VLAN , Segmentation, Remote Desktop, VNC.
- Cybersecurity, Asset, Cloud, LAN
- IDPS - Intrusion Detection and Prevention System. An acronym that refers to software that "watches" a network for unusual traffic patterns; usually to detect, log, stop, and report security incidents.
- IoT, IIoT, MES, Edge Device, LAN, WAN, VLAN, SSL, TLS, HTTPS, SCADA, HMI, DCS, PLC, PAC, Cloud, Layer 2 / Layer 3 Device, NAT
- Domains/Domain Management (ie, Active Directory, Permission often required to gain remote access)
- MES - Manufacturing Execution System
- ICS (industrial Controls System), Modem, Gateway, VPN Broker, 2FA (two factor authentication), Firewall, Inbound/Outbound, Network Segmentation
- Backdoor? Jump server?
- Remote desktop/desktop sharing collaborative sessions (Skype, MS Teams, etc.)
- Cloud - Delivery of data to on-demand computer system resources, without direct active management by the user, providing data access to all those with permission.

7 - We would like members to share learning experiences (positive or negative) on any of the topics above that may help others gain a better understanding. If you have one then please describe briefly.

- Some of the remote access VPN profiles have a large number RA users with access to a large number of whitelisted IP's. Becomes difficult to manage and increases chances for error. For example an OEM downloaded a PLC program to the wrong PLC. Worse than that it was a PLC at a different site — **Anthony Perea**

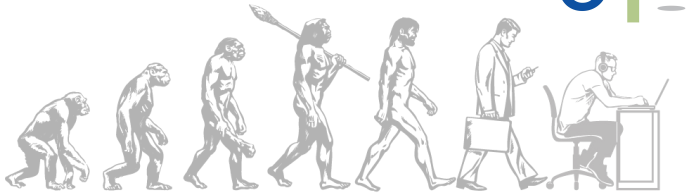
- We have been supporting some clients using Teamviewer to connect into the VSphere, all servers in the plant are virtualized so in the VSphere is configured the security and the access to some servers depending on the knowledge. This solution requires 1 Teamviewer license — **Juan Felipe Trujillo Ceron**

- Mostly positive. Changed ip of wrong server. Put PLC into momentary stop. — **Andrew ORegan**

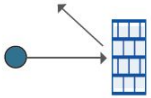
Q8 - Are there any subtopic that you would like to cover under this session?

- A digital maturity model and how to assess yourself and others in that model and use that as a basis to start from (see the next slide)
- Corporate Stakeholders that do not understand technology and Corporations with extremely tight restrictions
- The International IEC 62443 standards could be something referenced or at least mentioned in the best practices guide.

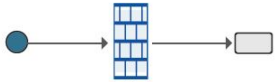
Stages of Connectivity in a Manufacturing Plant



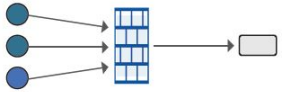
No external access outside the company



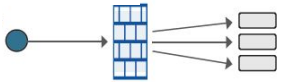
Limited "One to One" (IT allowing access)



Many to One system (multiple people to support one system)

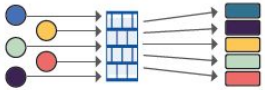


"One to Many" (Support of many systems such as OEM Machines)

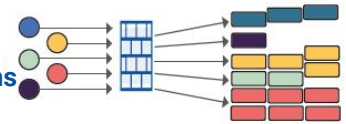


Plant recognizes value and expands the number of connections

Several connections for different systems



Many different connection to multiple systems



Complex Security challenges with many different systems poke holes in the firewall either IT or OT

Need for a single secure IT connection that is segmented and managed by OT to avoid external changes at inappropriate times. Need to record activity by individual and time.

Challenges in understanding what changes and who made them

Limited access to single person and asset

Higher installation costs and slower response times to issues

ISSUES

Next Questionnaire: IT Collaboration

- What activities have contributed to a positive outcome in your IT/OT interactions?
- What activities have created problems or issues in IT/OT relationships that should be avoided?
- What priorities are different with IT and OT?
- What are some of the key initial steps to create a better working relationship?
- Review and comment on the Maturity Model
- What are the challenges as an outside company when dealing with a customers IT group? If you are an end user, do you have recommendations for outside companies on how to deal with your IT team?

Thank you for your participation

Looking forward to seeing you online in fourteen days.

OMAC
The Organization for Machine Automation and Control

ei 3