The OMAC Remote Access Workgroup
Session 7

- 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

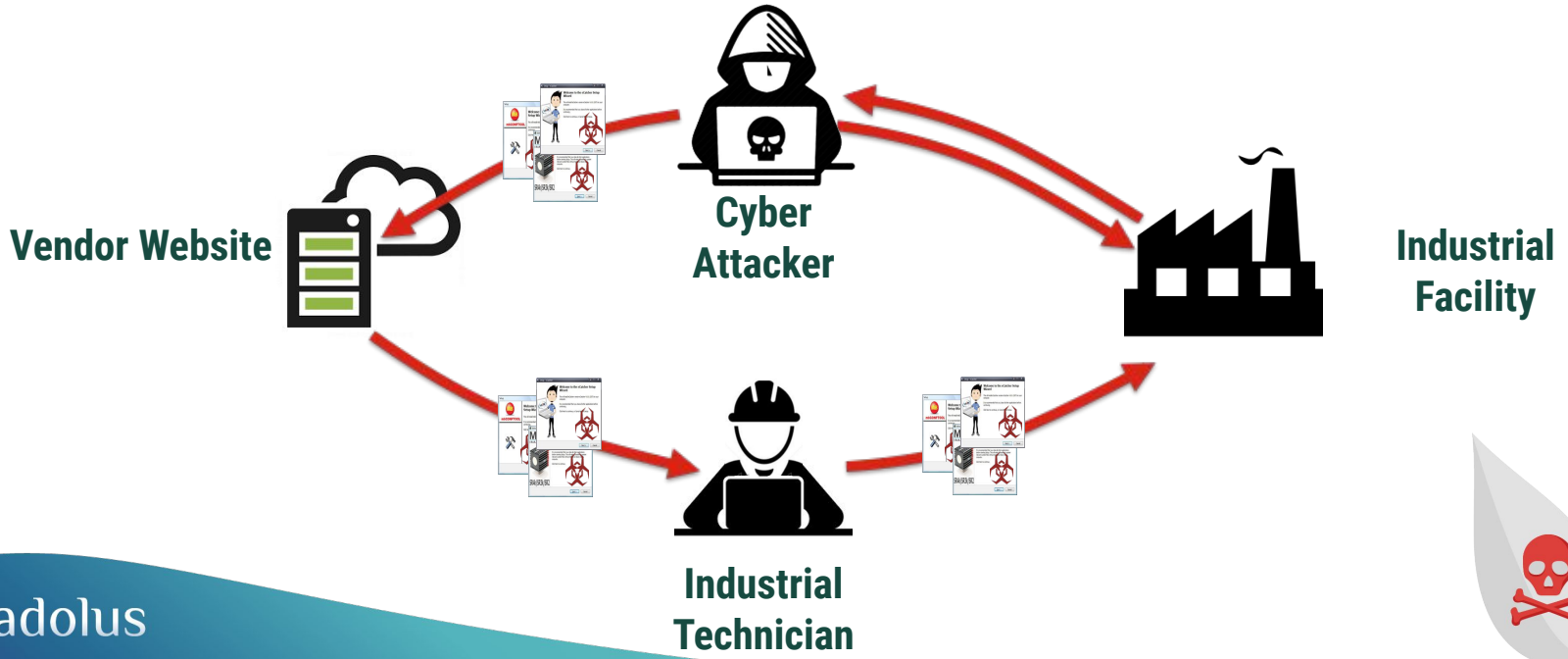
Eric J. Byres, P. Eng, ISA Fellow

eric.byres@adolus.com

- Recognized expert in SCADA/ICS and IIoT security
- Invented and commercialized the Tofino Firewall, the world's most widely deployed ICS security appliance
- CTO Security, Belden Inc. (2011-2015)
- Chair of the ISA SP-99 Security Technologies Working Group
- Represented Canada for the IEC TC65/WG10 standards effort
- Testified before US Congress on ICS Security of National Critical Infrastructures
- CEO of aDolus Technology Inc.
- **Not involved in any remote access product company**

Remote Access SW Modified by Attackers

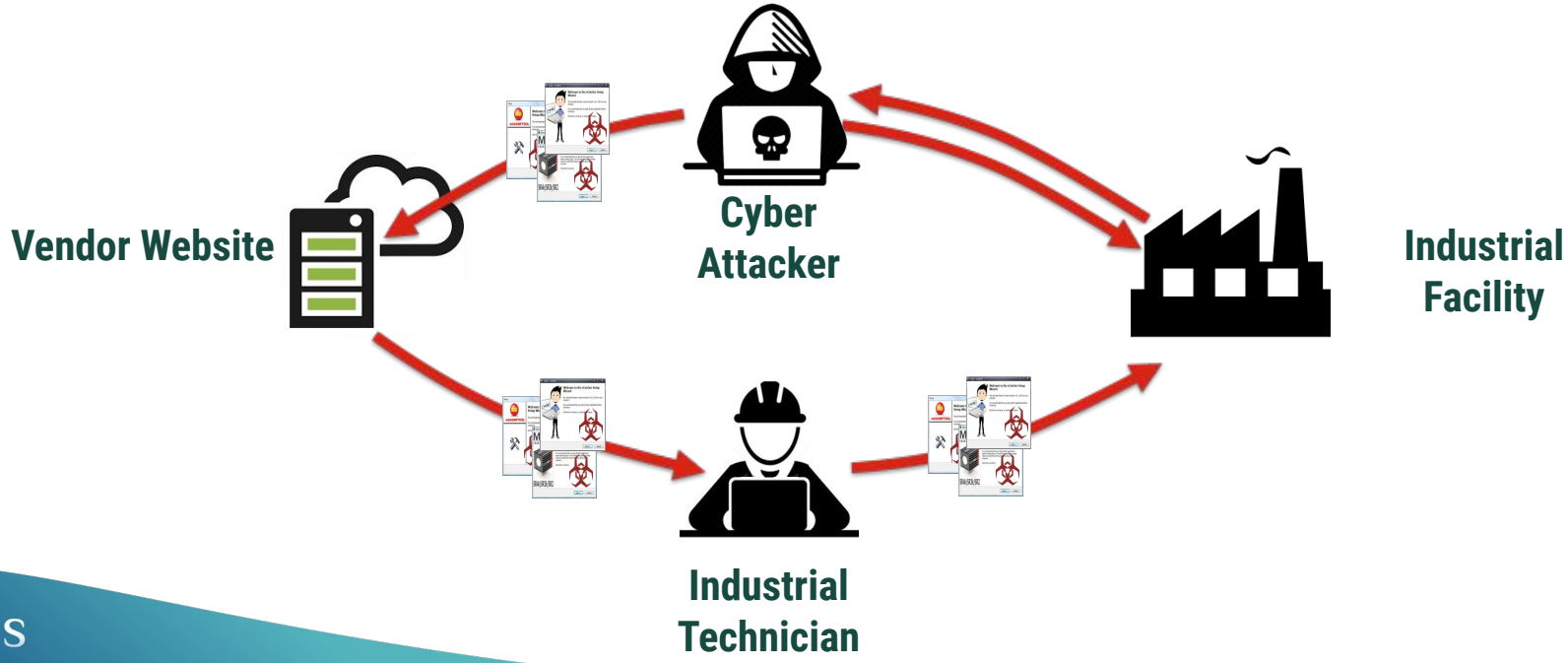
Dragonfly 2014: Exploiting Supplier-User Trust



adolus

Remote Access SW Modified by Attackers

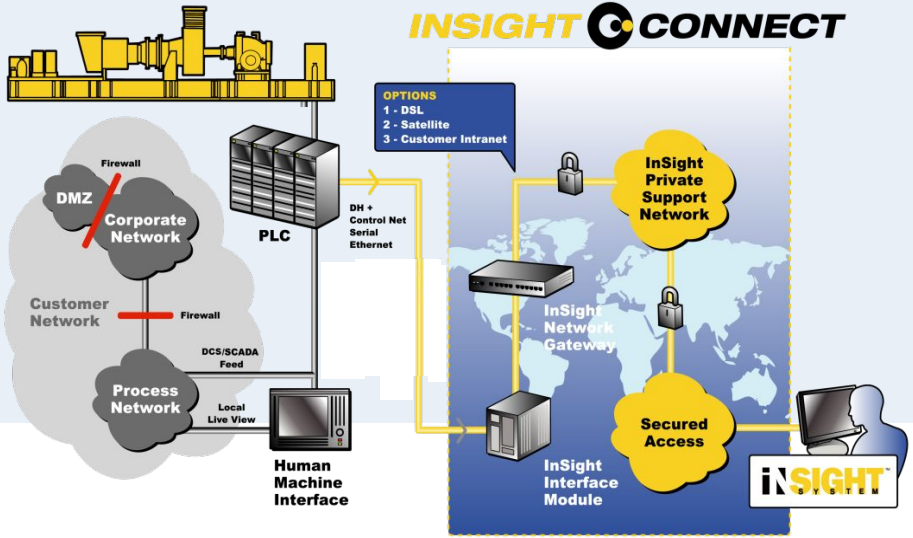
Dragonfly 2014: Exploiting Supplier-User Trust



adolus

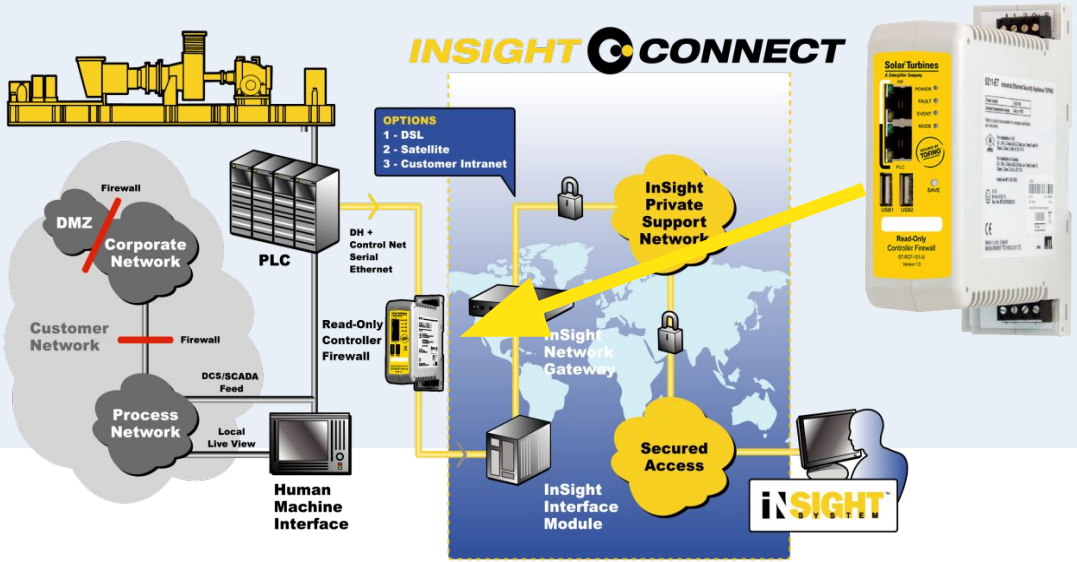
Securing Gas Compressor Remote Access

- Gas compressor packages are high risk systems
- BUT monitoring of platforms is critical in remote locations
- Risk of rogue insiders and unpatched vulnerabilities (even with VPN)



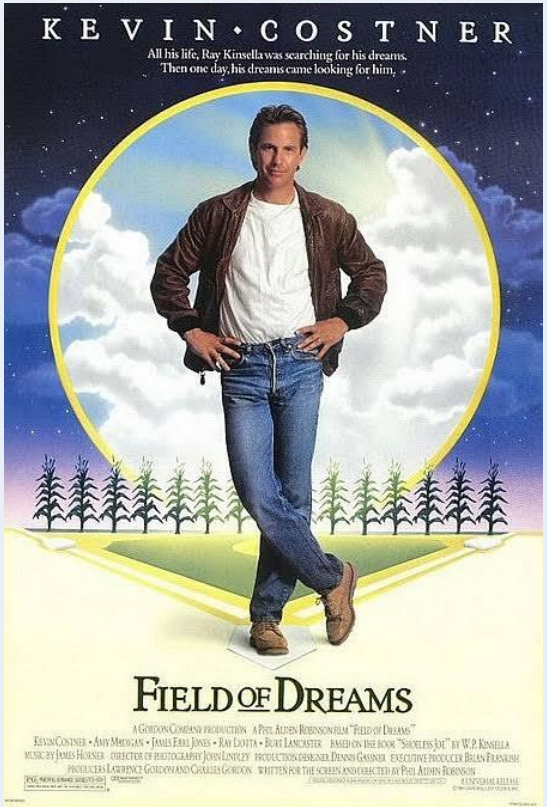
Read-only Controller Firewall

- DPI firewall inspects each SCADA message to ensure only data-read commands are allowed to the controllers

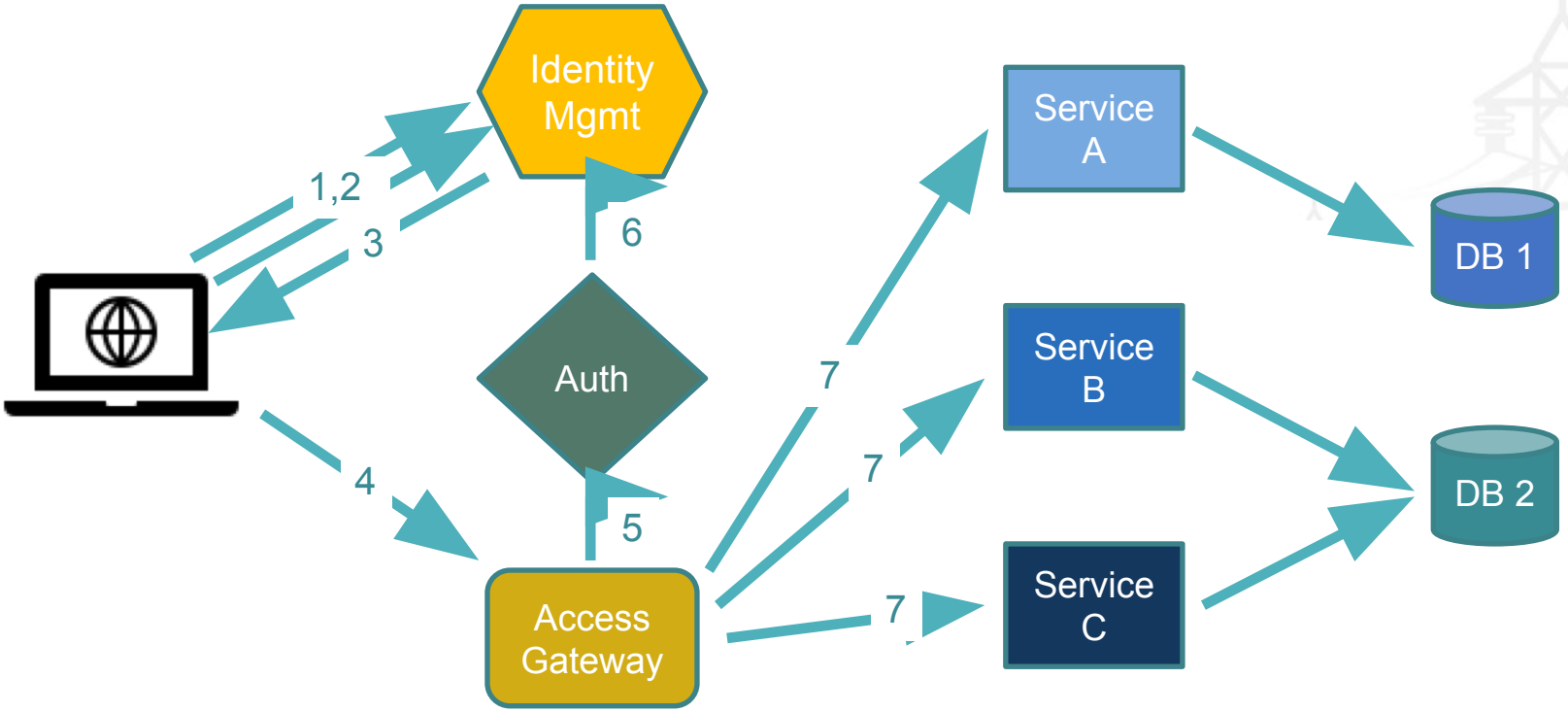


If You Don't Build It, They Will…

- Engineers are VERY creative…
- They will do whatever is need to keep the plant running efficiently

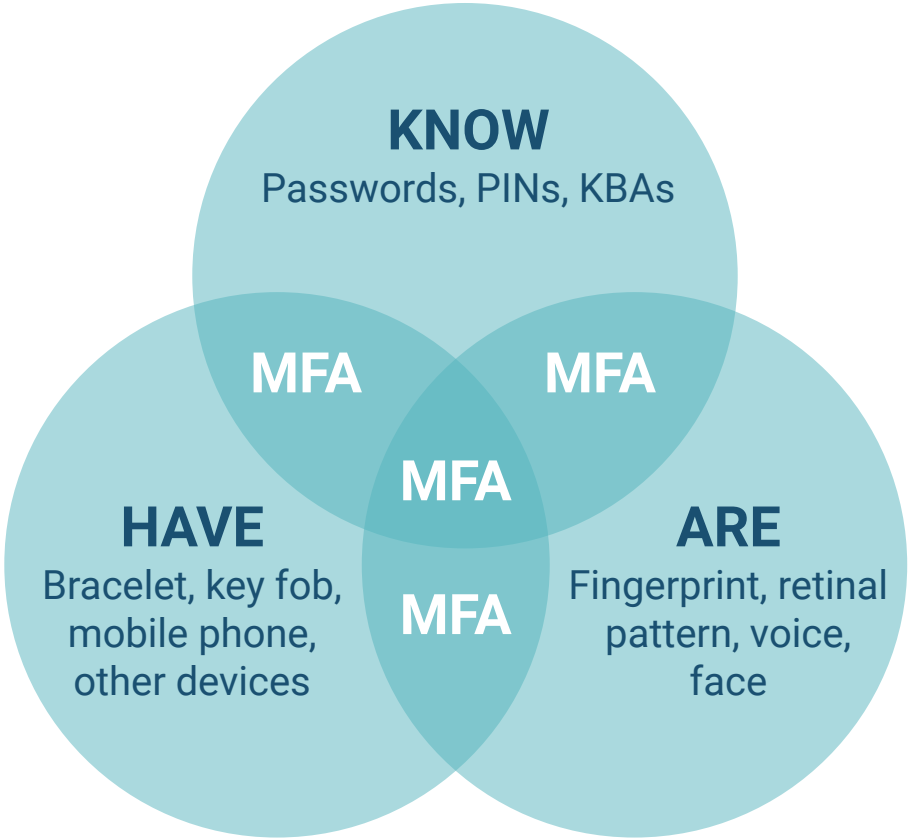


Separating Access Control from Identity, Authorization and Applications



Multi-Factor Authentication

adolus



Q1 - What details should be captured and documented when a remote activity occurs?

- Who connected, when they connected and disconnected, what devices they connected to, what protocols they used, who approved the connection, who was their "escort/proxy", notes about the actions performed
- User, session time (connect/disconnect), systems touched, change report
- Start and end of the remote activity, content of the activity as key points, next steps, planning of the next remote activity
- At minimum who connected and for how long. Ideally what they connected to and what changes were made, but this may be difficult to do automatically with some devices.

Date	Start Time	End Time	User Name	Security Level	Approval Admin	Agreemnt #	Device ID	Local escort	Reason	Actions performed	MOC Documentation

- Time and date. Who has accessed. Reason Devices accessed. How long. Changes and MOC documentation.
- Who did what, when and why. Also who approved and who accepted the outcome of the work
- Task to be undertaken, Risk Assessment, Start Time, Time to Complete, Rationale, Roll Back Plan, Usernames of Individuals, Src/Dst IP, Protocols, Remote Access Method
- User name who logs in, time and date. User IP address and / or MAC ID. IP addresses or devices accessed by the user.

Q2 - Should all individuals be required to fill out some information on the proposed action or reason before being allowed entry?

- **Provision should be made at some level for someone who will be providing ongoing support such as remotely commissioning**
- **An approver gets added into the cycle it's important to capture who is connecting to your OT systems and why. This information should be used to later assess if access is still required** If "emergency" access is needed - responsiveness should come from a more robust approval pipeline rather than riskier/less secure permission granting.
- Depends on the amount of the action; **differentiate between regularly remote access and one time remote access,** if an employee should have regularly a remote access, then I think it is not necessary, that s/he has to fill out every time some information
- Yes - it provides some insight into what is intended. **The disadvantage is it's an extra step (particularly if approval is required for the answer) that may delay the connection in an emergency downtime situation.** This information may also not reflect the real intent.
- Some documentation, even simple, **should be made to allow for a smooth system audit if there are issues**
- Yes, disadvantage is time, advantage is tracking and tracing afterwards
- Yes. Advantage - Audit trail. Forethought. **Third Party Remote Access Agreement.** Change Management. Disadvantage - Emergency response is hindered by paperwork. Additional time to complete works.
- **I think this is a good idea if it is done up front.** For example we may fill out a form that covers us for several months of activity including maintenance or troubleshooting. Many times our reason for connecting is for 'emergency' trouble shooting which it is difficult to plan for.

Q3 - What are some of the critical areas required to be recorded when applying “Change Management” in a Remote Access application?

- **Any changes that are made to controls systems.**
- **If this change is covering more than one specific department, then it should belong to critical area, which has to be recorded.** Or for i.e. if the change leads to a general change in the production process in a plant, this also has to be recorded.
- Who connected to what device. **Ideally the system would keep an as-found and as-left backup of the system so it could be determined what was actually changed** (and revert if the new changes cause a further issue after the connection is terminated).
- **Software and location of Software prior to change (initial footprint)** Changes both to the software and to the "Process Narratives" Software and location of Software after the change (new footprint)
- Logging, some form of impact assessment, some for of pre-job hazard analysis, some form of review/acceptance once the work is done
- Who(owner, stakeholder, approver), Why (current state, intended state) What , When and How,
- **Anything that requires Validation**. Some of our food and beverage customers are **FDA regulated and require Validation paperwork prior to and after making any modification to the control of the system.**

Q4 - Should there be security levels for individuals seeking access, and if so, how many levels should there be and why?

- It would be good to have some levels of security clearance, at least for temporary clearance access. **This would save a lot of unnecessary red tape and paperwork that can become really detrimental to timely service.**
- Yes, **individuals seeking to get access to secure systems or sensitive data should have additional approvals and verifications to ensure proper access to those resources**. Typically distinguish between contractors and business partners but varying numbers of permissions can exist within each of those classifications
- **2-steps (or even 3-steps) security levels**, where this access has to be checked from one or better two employees from higher ranking.
- Yes - I would think **one level with read access** and **one with read/write access would be sufficient**. On most devices there isn't a whole lot more you can do without making connection unworkable. You could also use levels to restrict what sort of devices the user can connect to.
- **At least 3 levels 1 High Hazard system access and changes 2 Production line access and changes 3 Data access. Diagnosis and troubleshooting. Software upgrades**
- Yes, **read only/able to change limited to a part of the machine that will be accessed**
- Yes. **Role Based Minimum 3 Levels** (User - Read Only, Maintainer - Limited Admin, Administrator) Least privileged is best practice but may not be practical pending site limitations
- **At least two levels. One for monitor / view only. A second for read / write / download ability**

Q5 - Should a separate and isolated network (VLAN or wireless) be created to link to plant floor devices without going over the existing control network?

- **That would be best practice. It is a more secure and controllable method, but it does have cost and complexity drawbacks.**
- **Yes. Separation enables easier and better control of access,** though the implementation can be more costly/complex.
- **Advantage is, that this isolated network is not able to disturb the existing control network.** Disadvantage is, that you are opening one more door through this alternative network to your plant. **It must fulfill some safety levels, then I think it is a good point to do it so.**
- **It would be nice, but may not be feasible for many of the devices**. Most devices we work with only have a single network port so you'll end up having some crosstalk anyway. **It's another layer that has to be managed.**
- Depends, for safety related machines a different zone is required
- **Yes if practical. Advantage - Grant specific access to required endpoints. Increased security and reduces risk.** Disadvantage - Extra infrastructure/equipment required and potentially limits scope to perform task.
- **There are advantages to this include allowing for more advanced network architectures and making it easier to segment and modify networks and prioritizing QoS.** The disadvantage I see is that **it can easily get 'out of hand'** where it is not documented well and no-one really understands how the network is set up.

Q6 - Do you feel that a cellular connection can be made and approved by IT? Are there ways in which an IT group can control cellular activity?

- **I think cellular is good potential fallback when other methods are ruled out**. I'm not aware of a good way to control cellular activity unless the customer controls the accounts.
- Not sure.
- **5G is coming, that's why we have to think about it.** IT can control with specific hardware these cellular activities, where upcoming connections are shown and where you can manage these.
- **I see cellular connections as a backup in cases where machines aren't networked**. I would be **concerned about using an always-on cellular connection into a plant network just to get around IT**. *If the connection runs through a managed switch IT could control connections.*
- **No.** Cellular connections to devices connected to any devices also connected to plant networks, even data. Some tanks that vendors supply and manage should be OK as long as level or pressure connected thru independent devices and I/O
- **Yes, in some cases there is no alternative** (e.g. elevator in middle of nowhere where network provider has bad service)
- **Connections should be approved in collaboration with IT & OT through appropriate change management processes**. Connection must be validated and certified to be using secure protocols. **Considerations for an "isolation switch" so remote site can control when cellular access is available and allowed.**
- I feel it should be approved by IT. **Controlling cellular activity may be difficult and defeat the point.** One way would be to have a cellular modem with a key that IT can used to enable / disable it on demand.

Q7 - Do you think that connection details can be captured automatically to make sure a base level indication of a connection occuring can be captured?

- **I think some information can be collected automatically. It's much more likely to be consistent and accurate if captured automatically.** I think if the traffic is going through a good router a lot of detail can be captured, but without human entered notes the context can be hard to deduce.
- **Yes. Useful to track user activity** for assessing need for access, also in reviewing incidence with possible association with remote access.
- **Yes, this is important. All connection details have to be registered automatically, so that you can follow all these activities from the history.**
- **That depends on how the connection is made. If it's made through a VPN or IT-managed connection it should be fairly straightforward** to log at least who logged in and the login and logout times. I believe windows authentication logs this by default. **This most likely won't occur for a remote desktop connection to a PC in the plant** (which is the way we connect to many customer machines today - the PC is on the plant WiFi and plugged into the machine of interest). I don't see any reason not to log the data if it's available.
- **Connection details should be captured automatically and stored in a log independent of the devices accessed. If possible changes should also be logged and stored**.
- **Everything that can be pre populated should be**
- **Yes - Through appropriate event logs provided it is enabled, captured, stored and archived accordingly**. Advantages - Audit Trail, Accountability Disadvantage - Additional storage requirements, log management and event retention, Standalone Systems
- **Some of it can be and should be.** As an integrator I feels that having a log of who connects and when **actually helps protect us from getting blamed for something that we didn't do.**

Q8 - What do you feel about the probability of a cyber attack happening over a Remote Access connection? Do you know any instances of this already occurring?

- **There are sufficient safeguards if proper procedures are in place and maintained.**
- **I feel very strongly that this an area of concern for all moving forward.** As industries mature, they will become an increasingly large target for cyber attacks. We're apart of what considered to be a slow industry. As we mature, more devices will be added online and there will be more incentives to attack our machinery and systems supporting it. In our industry, we've already had **one of our competitors hacked internally and was kept down for days meaning they couldn't service their customers or even provide new equipment.** If we were exposed and not able to support customer or even if the machines were exposed and customers were not able to operate them, this would be detrimental on several levels.
- **I know of no such incidents.** With remote access hardware only online/ plugged in when needed then **the risk is at zero**
- **I think it's inevitable that it will happen.** Unless proper precautions are taken it can be a very alluring target and there are always people ready to take advantage of those kinds of opportunities. I think there are a lot of things we can do to reduce the viability and the attractiveness of such an attack. I know of a customer who had a cyber attack but they weren't very forthcoming about how the attack happened or if it was related to remote support, though it seems from the actions they took afterwards there is a good chance it was related.
- **Increasingly likely and needs to be planned for**. No instances that I'm aware of yet.

Q9 - What do you feel about the probability of a cyber attack happening over a Remote Access connection? Do you know any instances of this already occurring?

- **Cyber attack will be always an issue, that's why updates and patches of remote access connections are important.** Personally, I don't know any instances.
- **It's definitely possible and largely depends on the security in place** and whether it's always available or just available on demand. I don' t know of any instances of this occurring.
- **If someone wants in they will get in**. Many times data is just collected and utilized. I have seen this in plants in Singapore being accessed for data from China sources. **We had a site that had corrupted SAP system and held for ransom. SAP was in the Cloud but some believed the cyber attack was generated thru the shop floor and up to the cloud. Most "cyber attacks" are self inflicted. Usually from IT untrained contractor sources.**
- It is possible but I am not aware of situations where it happened. Since we put a machine in place for 15+ years the remote access should be designed with the future in mind. Maybe the remote access system should be revamped or replaced every 8 to 10 years
- **Highly likely. From an adversary perspective, this is the most likely method of intrusion.** Ukraine Power Grid SCADA - Hijacked VPN sessions (2015)
- I don't know of any instance of it happening personally. **I feel that when they do happen is more often a case of people not following best security practices rather then a technical or network design issue. i.e. someone writing down a password on a sticky note.**

Thank you for your participation

Looking forward to seeing you online tomorrow.

OMAC
The Organization for Machine Automation and Control

ei 3