FPSA
Food Processing
Suppliers Association

FPSA – Technology Network
Technote – Bridging the Information Gap with Secure Remote Access

Access to the plant floor operations and the information it contains historically has been a physical activity. Management, suppliers, and support was done by going to the plant, and accessing equipment directly. With the need for remote access due to improvements and technology, and avoidance of non-essential personnel in plants, bridging this information gap with secure remote access is critical. This paper discusses the challenges seen by various suppliers.

BACKGROUND - Why this is a challenge.

IT and OT networks although similar in nature on general installation practices, have some drastic functional differences that end up creating challenges for accessing data and maintaining good network health.

Some notes on differences:

Enterprise IT Network:

- Typically, operational 8am to 5 PM, Monday through Friday
- Updates scheduled outside work hours.
- Most issues are on a single device in isolation.

Production – OT Network:

- May be operating multiple shifts, up to 24/7/365.
- Network outage results in loss of system control
- IT and plant managers need to work together to define objectives and identify risks.
- Downtime must be scheduled, months in advance.
- IT needs to understand underlying plant processes.

Enterprise Networks

Grown with direction as part of a capital investment; planned and future proofed.

Industrial Networks

Piecemealed together as quickly as possible to avoid downtime; upgraded as needed.

TECHNOLOGY
NETWORK

CHALLENGES – What Roadblocks do we run into with OT and IT networks?

As part of this technote, information based upon multiple disciplines of users affected are listed with their individual challenges.

End Users: These are the factories that run the food processes that are directly affected when their plant is isolated from resources, as well as needing to ensure the plant floor is protected from outside intrusion

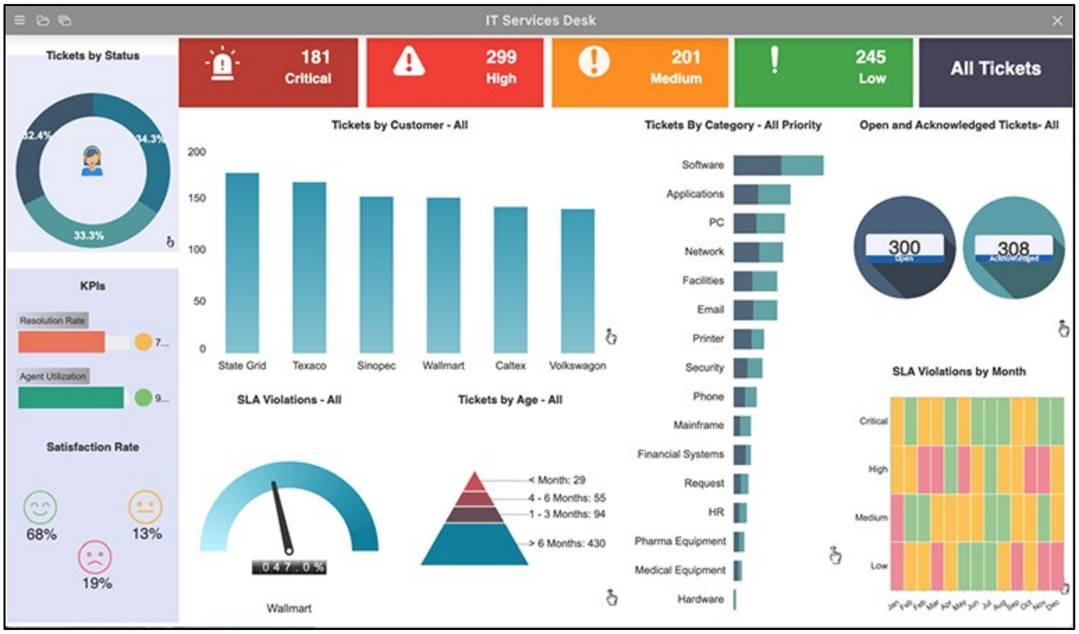
OEMs: These are the equipment manufacturers that have a direct stake in the game to ensure their equipment is running optimal for the end user

Software/Automation Vendors: These are the implementors of the software that runs the factories, and typically responsible for the uptime of the plant from a technology perspective

End Users:

Stakeholders need information about how their operations are running. If they are not at their plant, accessing information that is important to make operational decisions and improvements. Some challenges from End Users:

- Dashboard access – historically, dashboards run on a large monitor on the plant floor – when working remote, access to these dashboards is unavailable.
- Operation Reports – without cloud hosted data, there is reliance on emailed reports that may not be real time.
- Uptime – without suppliers having access, uptime can be compromised.



Along with the information needed by the End Users, the system also needs to stay secure. Connecting a control system to the internet directly can have detrimental affects if the system gets compromised, as we have seen with multiple cases of ransomware throughout industrial operations.

FPSA – Technology Network
Technote – Bridging the Information Gap with Secure Remote Access

➢ OEM's – Equipment Manufacturers:

OEM's want their equipment accessible for remote diagnostics, and remote support to minimize customer downtime and more efficiently use scarce service team resources. OEM's are typically stand-alone pieces of equipment, so connecting to these pose some additional challenges, but can also produce the most information that would be needed for optimizing operations.

Challenges OEM's encounter:

- Some customers do not want to keep their equipment connected to the network 24/7.
- In some cases, IT support is offsite from the equipment, which causes delays if physical network issues arise.
- If we can get the equipment onto the customers internal network, we still need to somehow gain access to the plant network from outside. Which means we need a secure entry point into the customers network which is controlled by the plant /company IT group.
- We have seen long delays when trying to upload or download programs in certain VPN gateway services.
- Cell phone network interfaces are available, but can be expensive to use long term.

In some cases, special equipment is installed in the equipment to allow communication to the plant networks. NAT [Network Address Translator] is one solution many OEM's provide within the equipment switches to make it easy to tie into any existing Ethernet Network Address scheme.

Some of the hurdles of implementing this are:

- Many plants don't provide sufficient network address information to allow a proper setup of a NAT.
- Some locations want nothing to do with a NAT or a complex managed switch in the equipment.

Data collection within the OEM space is important for OEE or other data to determine operational performance. The challenge is not only in accessing this data, but the data types that are trying to be gathered in many cases are either configured differently per machine, or is not being collected in a manner that would provide actionable information.

- A prerequisite to data and conditions for digital networks reside in the configuration of information from older version assets compared to the same category of equipment in a newer version. Some machines may be programmed with PackML and others not. The opportunity exists to help the end customer and equipment supplier define how the line or equipment operates enabling the correct tag conditions for the Production OT and IT Networks. (if this is solved access to the data will be an easy conversation with IT and Operations)
- Sensitivity to production fault data in real time. If production facilities encounter some SKU's that are more challenging to run the equipment data could be skewed being identified as a bad actor when in fact inefficiencies are in other areas. (example: not conducting maintenance as recommended by the supplier and uncontrolled variability in other areas)

➢ Software/Automation Vendors:

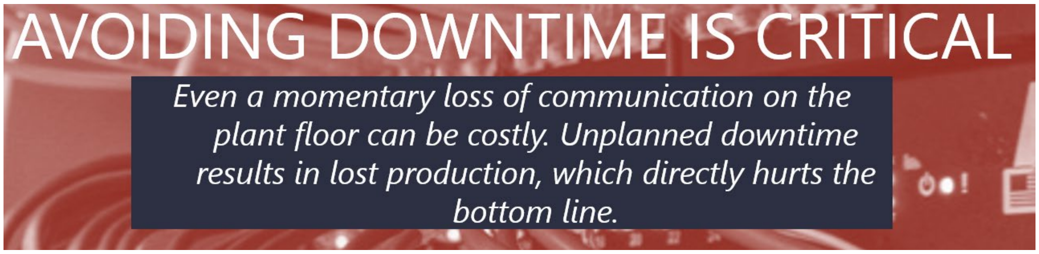
Software and automation vendors are typically responsible for ensuring a plant remains in operation, either by remotely supporting the day to day activity, or keeping software and operations up to date to eliminate vulnerabilities within the system. The biggest challenged faced by software vendors is maintaining a proper level of support

Support:

Support for operations is key for many food processing facilities that run 24-7-365. Uptime is critical to ensure production gets out and food safety is maintained.

Some of the issues encountered by support have been:

- Air Gap OT Implementation – this is a design that completely separates IT and OT infrastructure. While this eliminates access to the internet from the plant floor, it also eliminates remote support access.
- Insecure implementations – to get support if a plan with IT is not established, back doors are frequently created to ensure uptime. Items like dual homing servers (multiple network adapters to communicate between separate networks), direct internet access to the plant floor, or other undocumented remote access methods are cause for security concern.



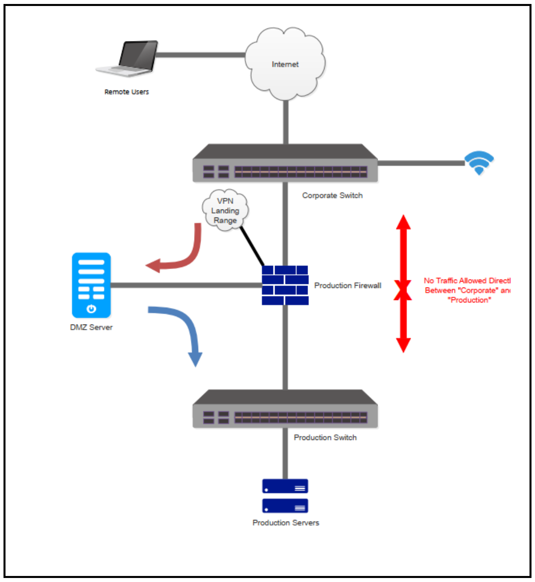
AVOIDING DOWNTIME IS CRITICAL

Even a momentary loss of communication on the plant floor can be costly. Unplanned downtime results in lost production, which directly hurts the bottom line.

FPSA – Technology Network Technote – Bridging the Information Gap with Secure Remote Access

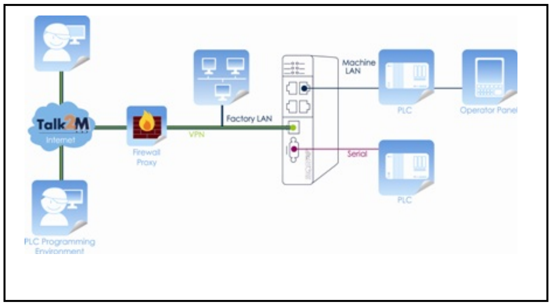
SOLUTIONS – Methods for Access

A key item to note is there are various options for secure access – but it must be coordinated with the end users' IT team, and an OT Network expert. Rules in the OT environment from a network standpoint are different than what applies in the enterprise network. Some Solutions:



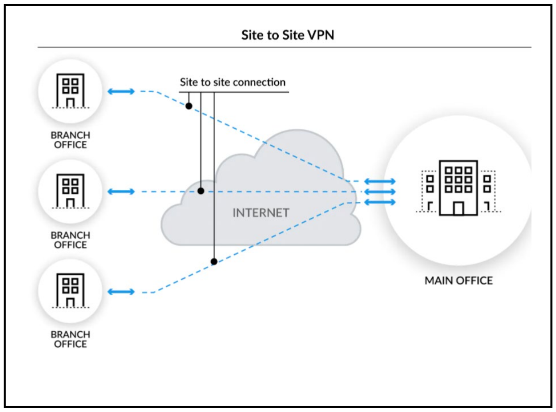
- **DMZ Implementation managed by OT provider:**

By far the most secure method to have two-way traffic between the enterprise layer and the industrial layer. This follows the Purdue model as a best practice. This needs coordination between an OT Network services provider and the end users' IT department to make sure items are configured properly for both sides.



- **Industrial M2M communication:**

This typically is a VPN appliance that is configured for specific access to a machine – if implemented with approval from the Plant IT department, can be a solution for individual pieces of equipment, but if installed without ITs knowledge, are typically viewed as a back door, and eliminated when found.



- **Customer Managed VPN:**

Very standard method for remote access but follows many of the standard enterprise IT rules. Getting access approval or updates can be a slow process depending upon the customer IT department, which can extend downtime. No support after hours in most cases if there are issues.

Conclusion - How Secure Remote Access helps the customer and technology suppliers.

1. Security: Keeps the plant floor from unauthorized access - simply stated – you don’t want to be in this situation.

2. Uptime: Remote access for key vendors when controlled properly – troubleshooting a system without travel requirements can save hours of downtime
3. Data: Data for the stakeholders, data for the OEM’s, data for process improvements. All of this data when configured correctly and securely accessed can improve a plants productivity.

Coming Next: A deep dive into the DMZ structure – can this work for you?