End to End Security

Achieving End to End Security in an Industry Lacking Interoperability

www.OT-MES-IT.com

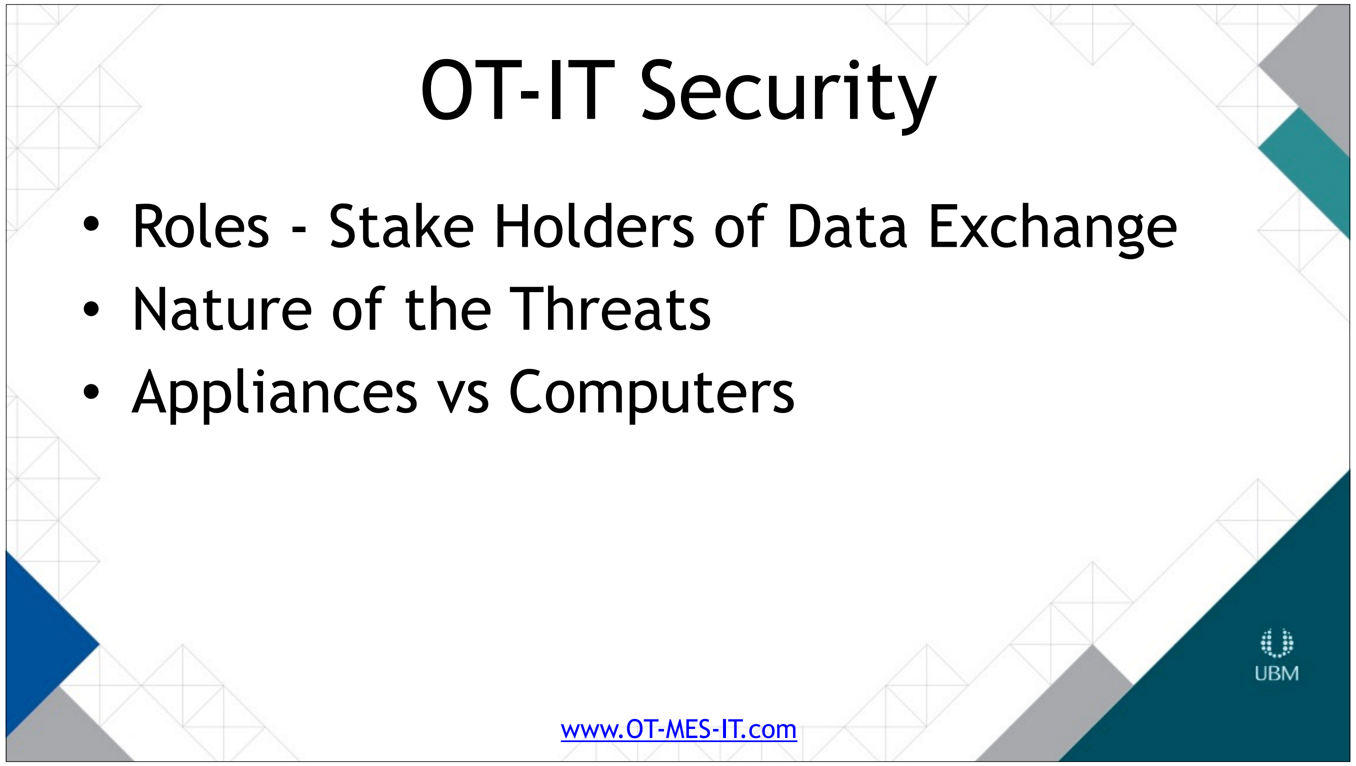
Introduction

Questions and Answers

#OTMESIT

www.OT-MES-IT.com

For Q&A use our hashtag #OTMESIT on Twitter for ongoing conversations.

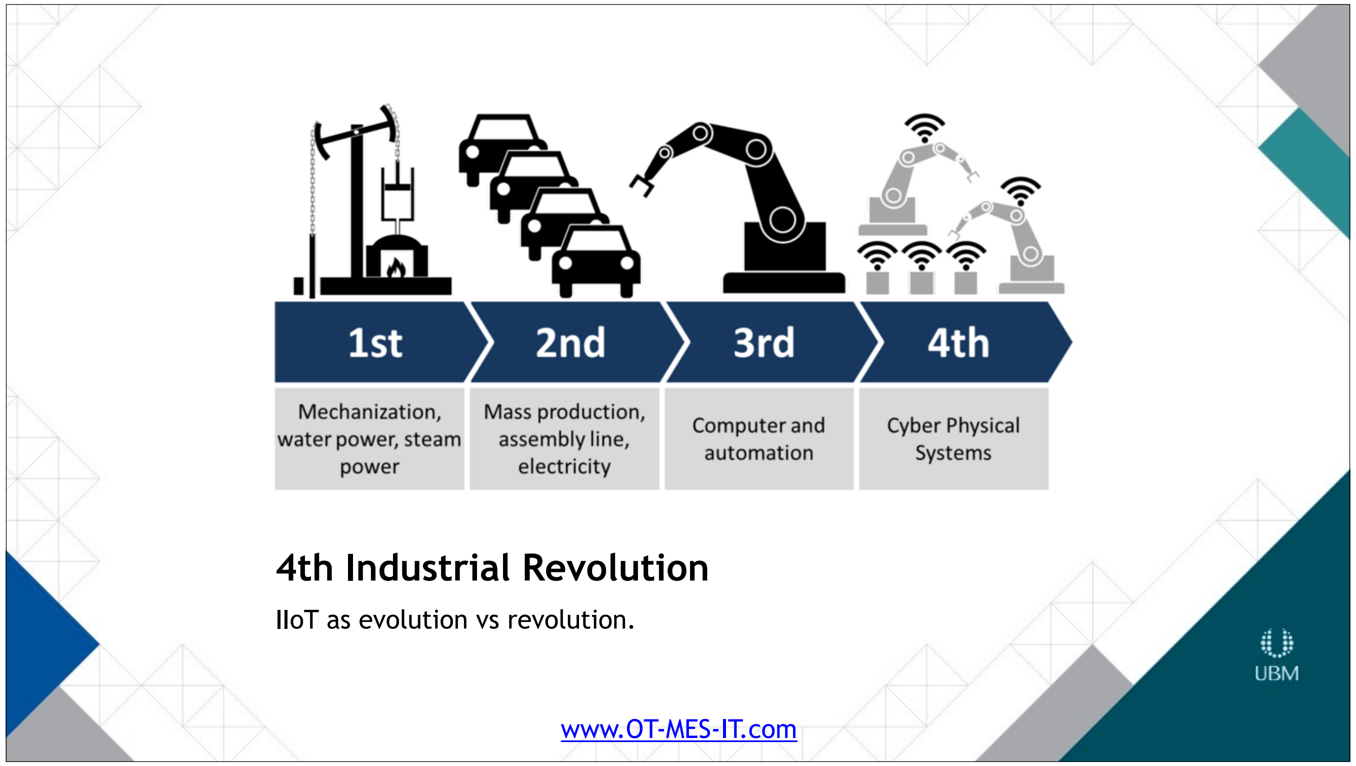


OT-IT Security

- Roles - Stake Holders of Data Exchange
- Nature of the Threats
- Appliances vs Computers

www.OT-MES-IT.com

1. Roles - stake holders of data exchange
2. Nature of the threats
3. Appliances for OT and IT security.



1st	2nd	3rd	4th
Mechanization, water power, steam power	Mass production, assembly line, electricity	Computer and automation	Cyber Physical Systems

4th Industrial Revolution

IIoT as evolution vs revolution.

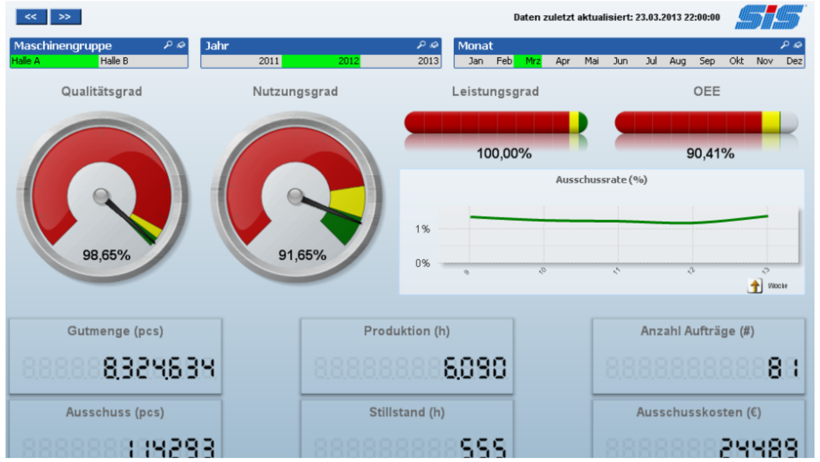
www.OT-MES-IT.com

Our workshop is going to teach how an MES gateway appliance will radically simplify Smart Manufacturing deployment.

Who’s ready for the next big thing? Who would like to see the payback on their investment from the last big thing?

IoT is not necessarily a new concept. It used to be called telemetry or data acquisition or supervisory control. Very few in industry plan on sending their proprietary sensor data to the cloud instead of to a machine’s PLC, but there is profitable opportunity in Smart Manufacturing. Manufacturers can use their existing technology to improve monitoring and control, and deploy manufacturing’s data communications more broadly… if it were connected correctly.

A dedicated MES gateway appliance used to connect manufacturing’s Operational Technology (OT) with administration’s Information Technology (IT) eliminates PCs and OPC middleware from the factory floor, and all of the complex and compromising connection issues that come with them.



PRODUCTION MANAGMENT

MES - Manufacturing Execution Sytems

UBM

www.OT-MES-IT.com

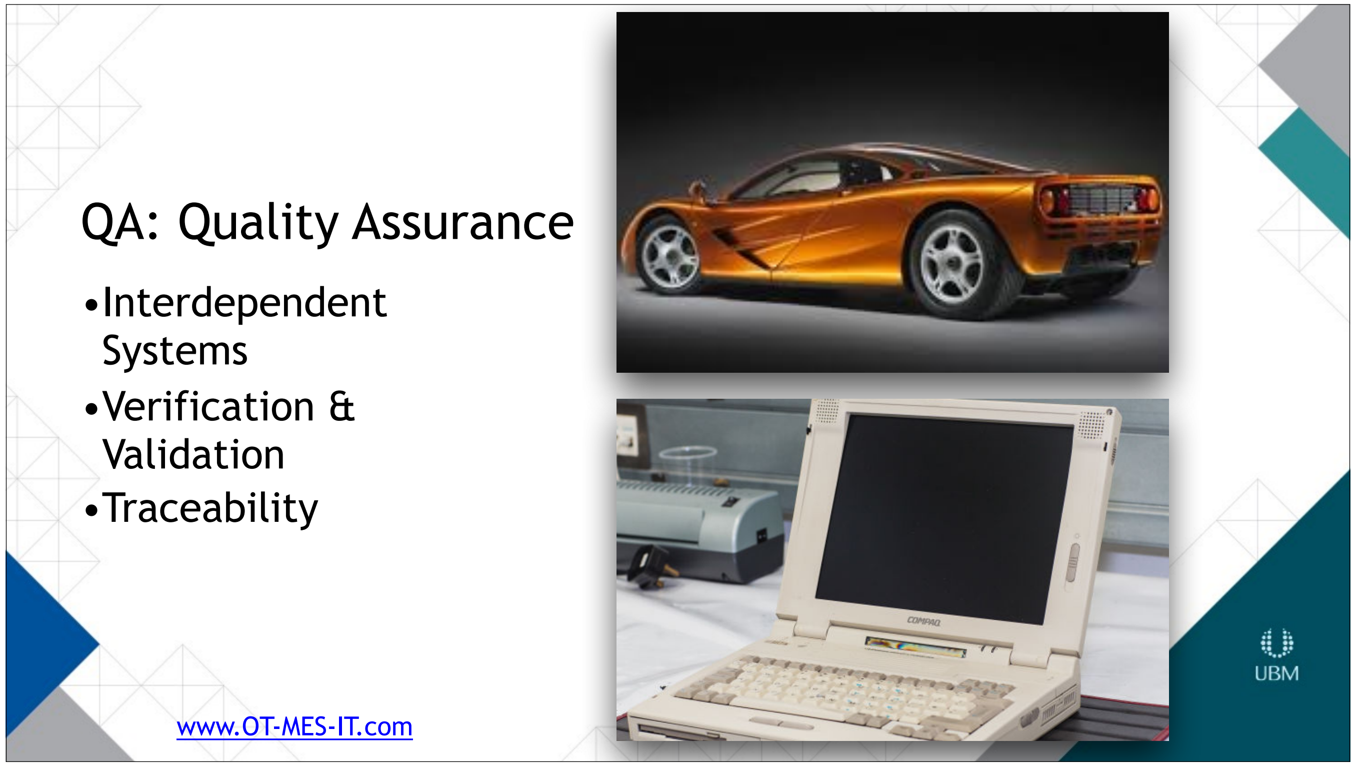
How many managers are in the audience?

Manager's, I want you to be honest with yourself - did your pulse beat a little faster at the site of a dashboard? I mean c'mon, it's all of product development and production analysis at your fingertips!

Why shouldn't you expect production data this way? We traveled here with pocket sized devices that allow us to work anywhere we choose. Today we chose to work in Anaheim, but we didn't disconnect from our office while we're here. So why is it so hard for a production manager to have the same simple connection with their production floor?

PCs on the production floor are preventing the acquisition of the production data (MDA) you need to meet your goals. Engineers responsible for OT, and IT professionals responsible for system administration cannot take ownership of a PC on the production line, because of the natural conflict between the two systems' responsibilities and expertises.

You may be asking how can a $148 billion medical-device industry, filled with talented and educated professionals not be able to find an easy connection between OT and IT when the information is needed so badly and so justifiable?



QA: Quality Assurance

- Interdependent Systems
- Verification & Validation
- Traceability

www.OT-MES-IT.com

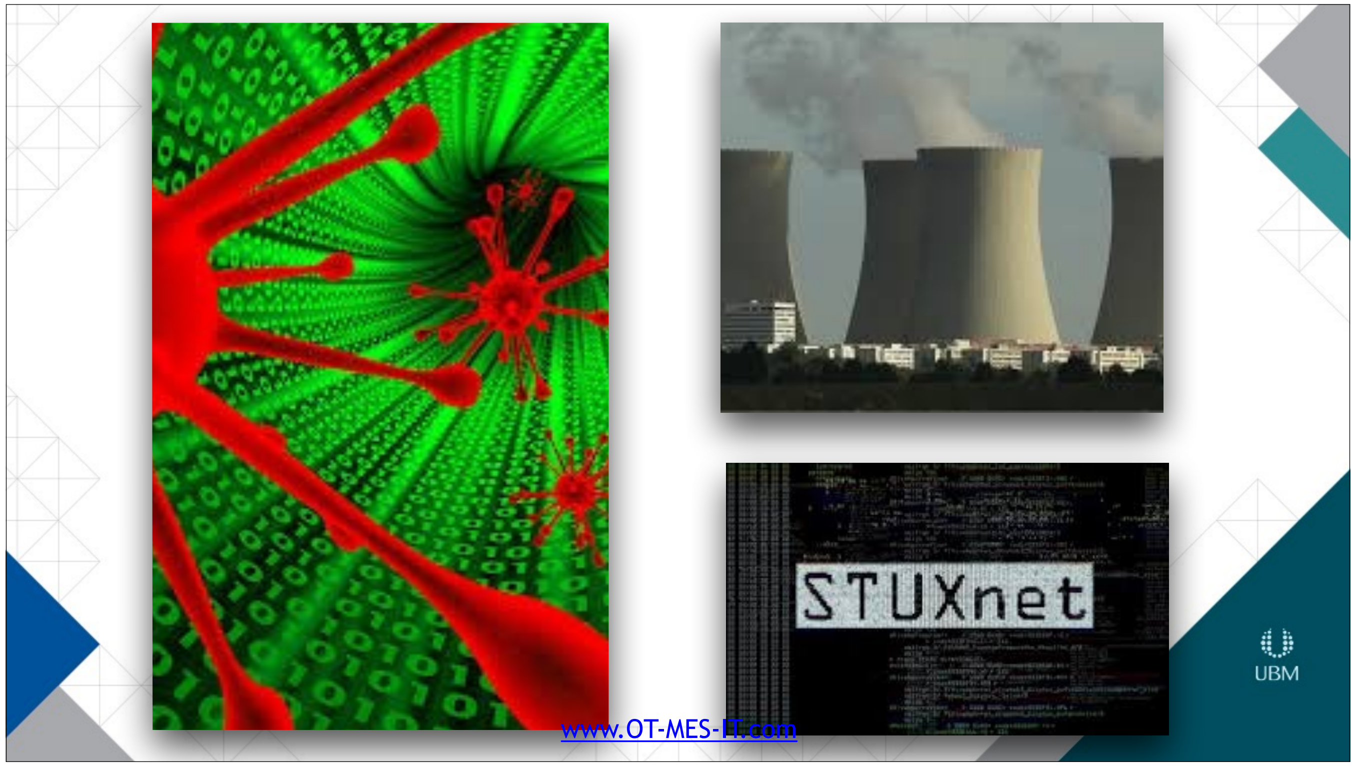
How many engineers are in the audience?

This is a $13M Mclaren F1 supercar. It's controls are totally dependent on a made-to-order CA card in a Compaq ~~LTE 5280~~ laptop from the early 1990s. ~~That Compaq is running a made-to-order CA card, and if you're lucky, you may be able to find one on eBay.~~

To most people, this news is an absurd story of incompetence. To engineers in process and production, it's common place. Process and quality assurance are ensured through systematic methods to maintain defined control parameters. Once they're in place, processes are not to be tinkered with.

All components of a production line that are passing and failing parts rely on decades of legacy automation solutions. Each device used in production is part of an interdependent system. Systematic methods maintain defined control parameters for process and quality assurance.

Any component to be added to the process must comply with the web of solutions that engineers are responsible for, and not interfere with engineers' production QA responsibilities.



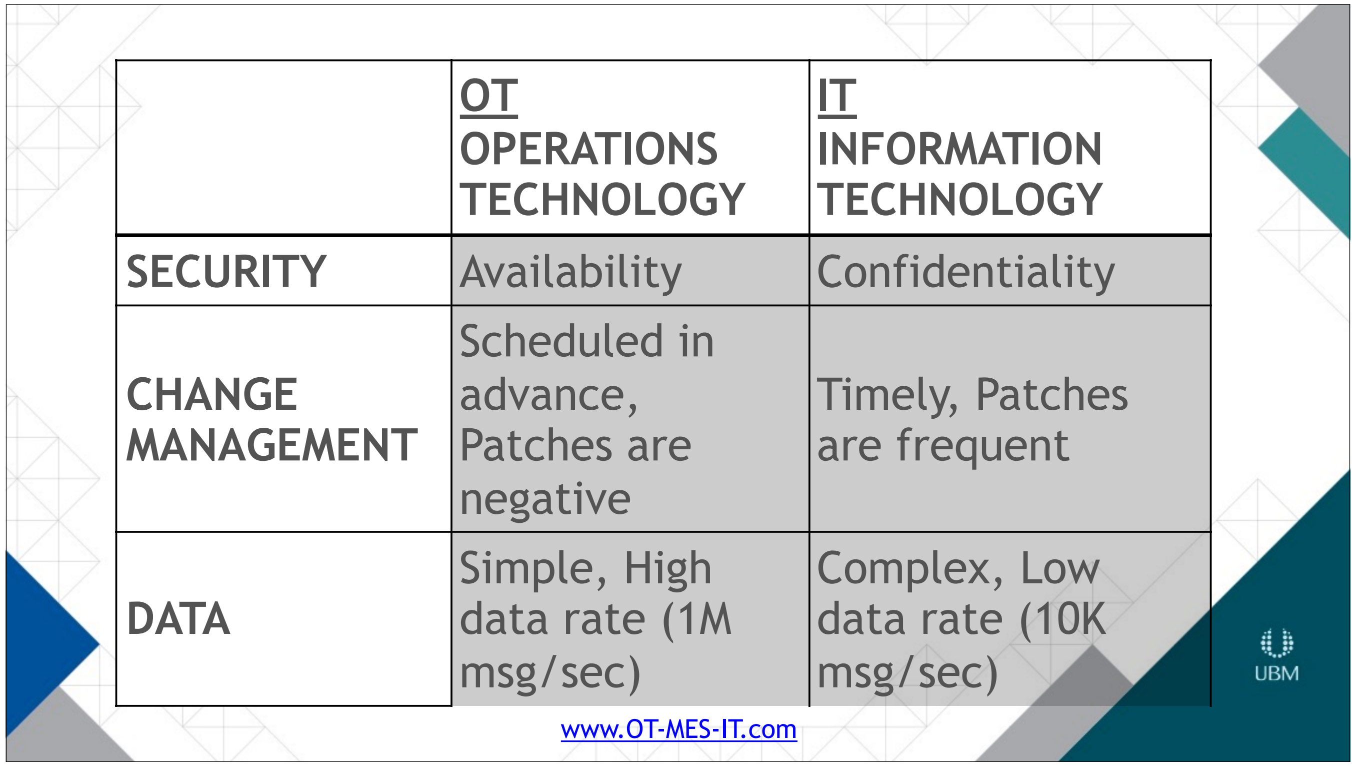
www.OT-MES-IT.com

How many IT professionals are in the audience?

In June, 2010, a tiny company in Belarus received a complaint about a software glitch. Detectives found a virus named Stuxnet. Unlike viruses and worms on the internet, this one was not trying to steal passwords, identities, or money. It crawled from computer to computer, around the world, looking for a network using a specific type of equipment - a Siemens S7 300 PLC. The virus was designed to speed up the motors that control nuclear plant centrifuges past what they're meant to be, and damage them. Operators couldn't see any damage because the virus was disguised from supervisory control (PC-based SCADA).

System Administrators have 2 problems: 1) dumb users 2) smart users.

Any PC in the organization is a security risk. The dominant and accepted technologies for implementing communication with ~~the~~ controls and automation on the production floor are 1) proprietary PC software and 2) OPC middleware. Either of these solutions are a security problem for IT because they're responsible for every PC on their network. Any PC is a security risk and must be managed to avoid hacking and system errors.



	OT OPERATIONS TECHNOLOGY	IT INFORMATION TECHNOLOGY
SECURITY	Availability	Confidentiality
CHANGE MANAGEMENT	Scheduled in advance, Patches are negative	Timely, Patches are frequent
DATA	Simple, High data rate (1M msg/sec)	Complex, Low data rate (10K msg/sec)

www.OT-MES-IT.com

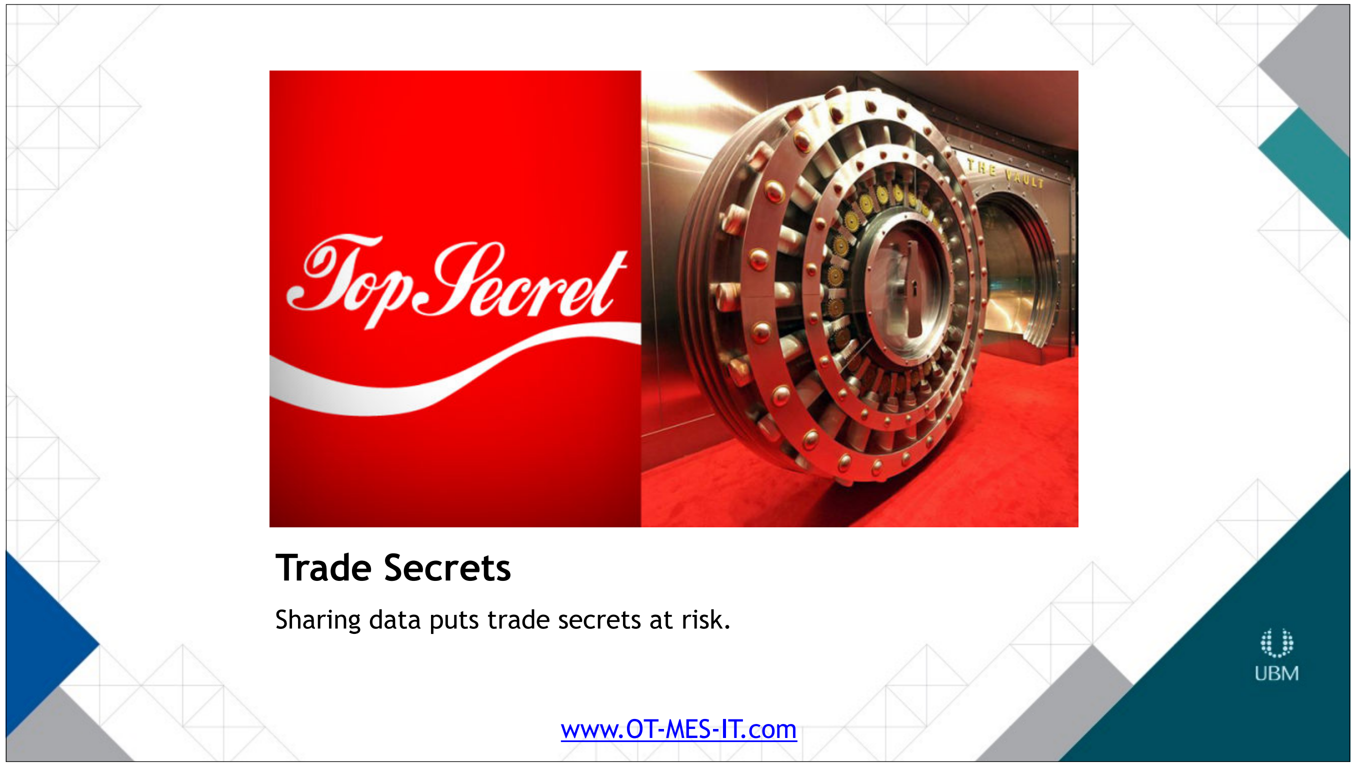
At this point, how likely does it seem our production managers are going to get their dashboard? No admins want the security problem of an engineers' PC entering their IT network, and no engineers want the process and QA risk of the office's PCs on their OT network. But why? Aren't they both hyper-diligent about the data integrity of their networks?

Both disciplines manage security, change management, and their data differently, and the expertise of one is in direct conflict with the expertise of the other. Security in OT means making sure the production is always available and online. Security in IT means total and complete confidentiality.

Changes in OT are discouraged and infrequent. When changes are required, they're scheduled a long-time in advance to plan production accordingly. IT must make constant, and immediate security patches to protect the network.

OT's ON/OFF machine data is simple, but runs at an extremely high rate to coordinate production processes in real-time. IT's data consists of complex operating systems and updates that run at low data rates in comparison to OT's.

Smart Manufacturing has been made difficult because companies are trying to converge systems that should be isolated from each other.



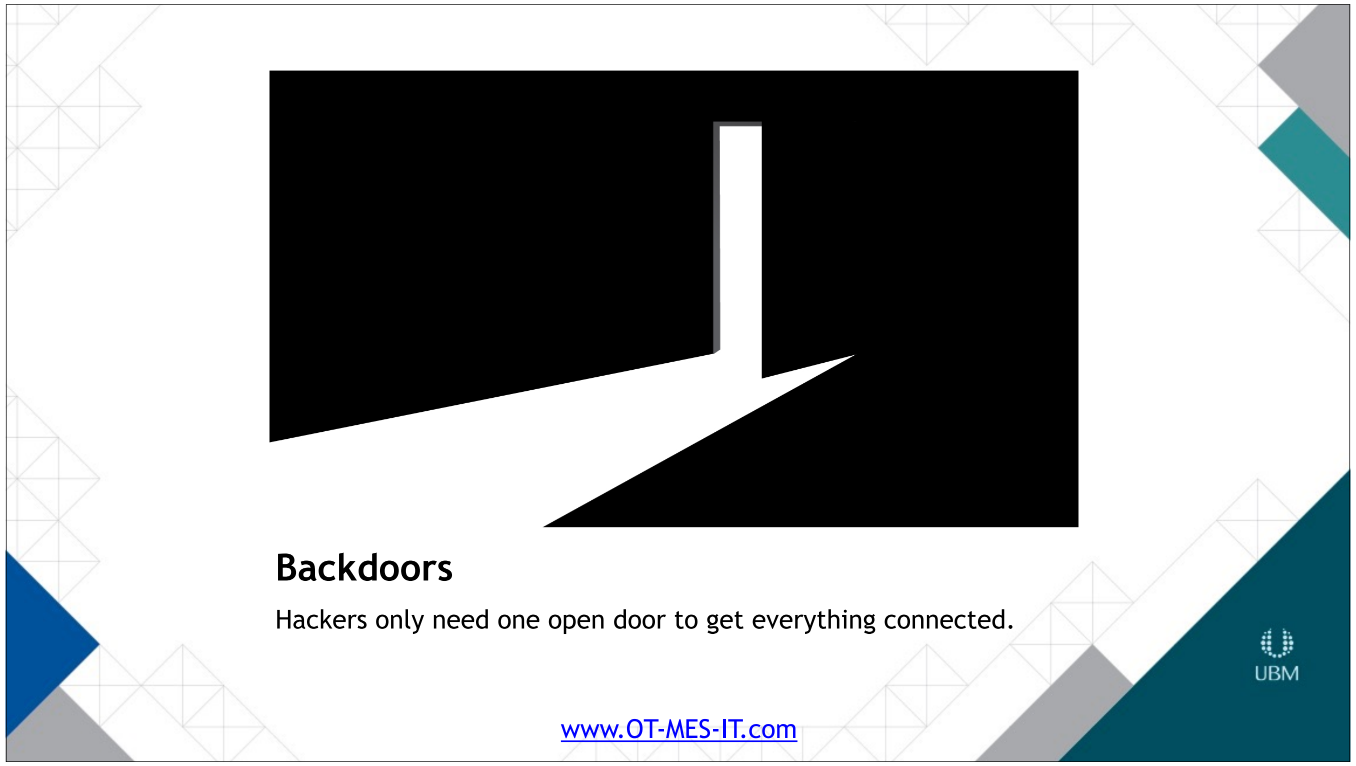
Trade Secrets

Sharing data puts trade secrets at risk.

www.OT-MES-IT.com

IT protects internal servers behind firewalls, double authentication, DMZs, etc.

The balance is between totally locked down and being able to function. The same way web servers are open to attack, so will web services next to industrial processes.



Backdoors

Hackers only need one open door to get everything connected.

www.OT-MES-IT.com

A backdoor in software or a computer system is generally an undocumented portal that allows an administrator to enter the system to troubleshoot or do upkeep. But it also refers to a secret portal that hackers and intelligence agencies use to gain illicit access. https://www.wired.com/2014/12/hacker-lexicon-backdoor/

Door Analogy:
If you have three doors locked and secure, but the fourth door is open, it doesn’t matter that the other three are locked. A hacker can enter the entire connected system through the one open door.

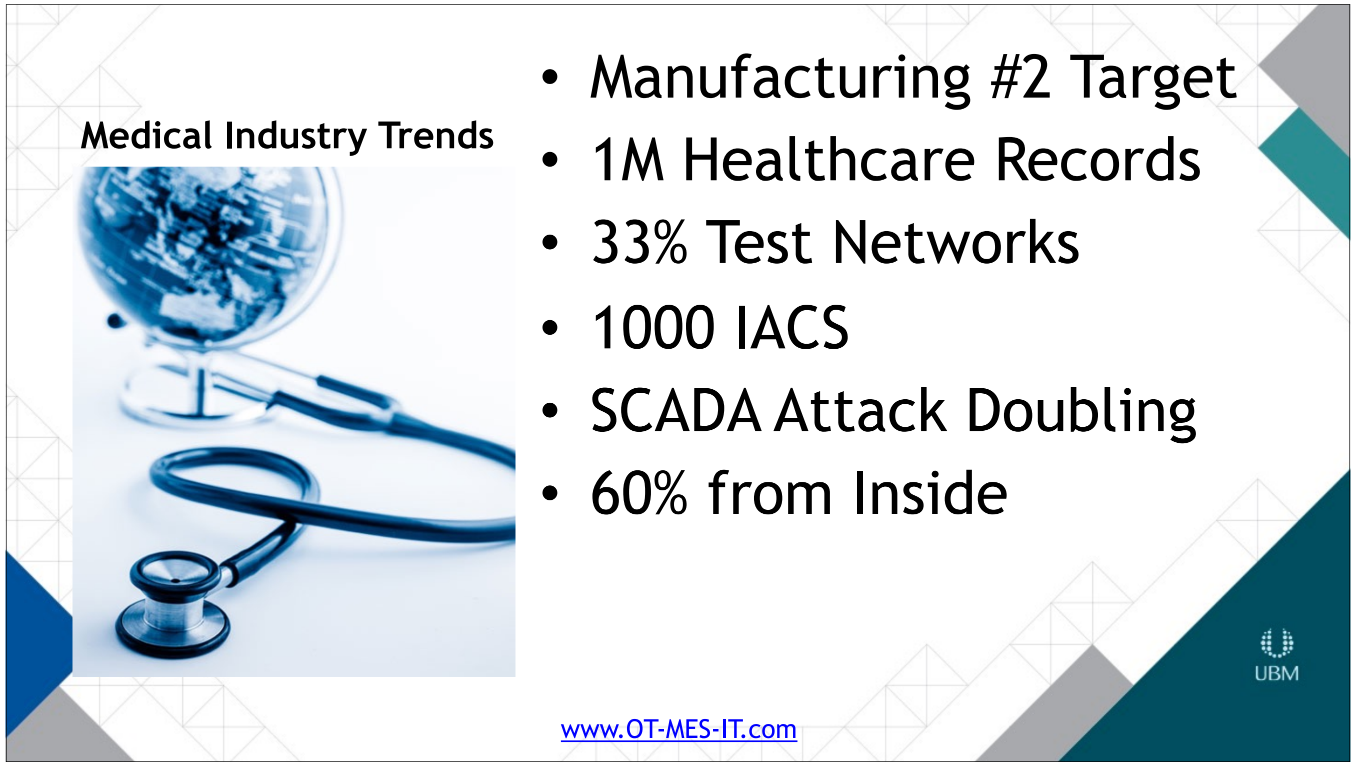
www.OT-MES-IT.com

What is an attack?

All of these examples are the result of flaws in Windows or outdated OS or a weak link in the network. They could not have been avoided - their vulnerabilities are built in.

If the OS is known, the vulnerabilities are already known and can be exposed.
-Windows XP on Target cash registers
-DDoS on Dyn to block popular sites like Netflix
-Phishing email messages to DNC to attack Windows and Adobe Flash vulnerabilities.
-flaws in Gmail authentication allowed hackers to take over an existing account
-Citi’s website was hacked with parameter testing or “middle man” attack to gain account information through the browser.

Hackers will always target the weakest link in the chain, where they can get the biggest bang for the buck. Meanwhile, the problem is, the infrastructure supporting the internet consists of a series of interlinked servers and cloud services, and no single entity has the power to vet and implement security for the entire chain.



Medical Industry Trends

- Manufacturing #2 Target
- 1M Healthcare Records
- 33% Test Networks
- 1000 IACS
- SCADA Attack Doubling
- 60% from Inside

www.OT-MES-IT.com

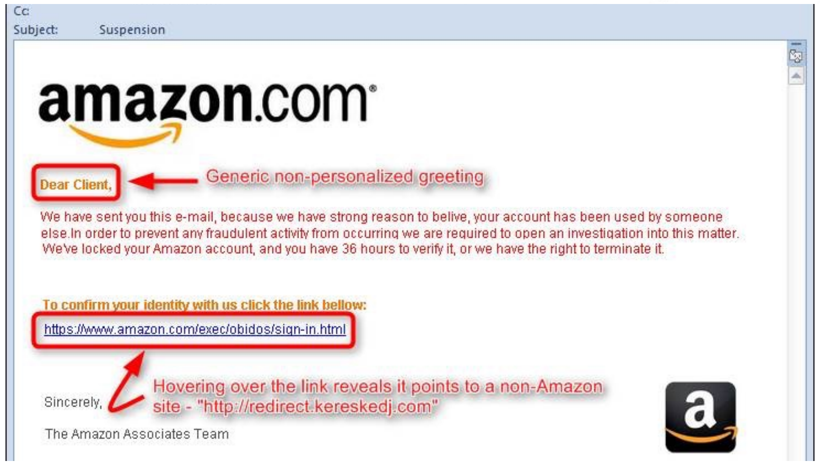
Manufacturing is the Number 2 target, accounting for 24% of all cyber attacks (Symantec). According to studies by the Manufacturers Alliance for Productivity and Innovation and IBM, nearly 40% of surveyed manufacturing companies were affected by cyber incidents in the past 12 months, and 38% of those impacted indicated cyber breaches resulted in damages in excess of $1 million.

Healthcare became the Number 1 in 2015, so medical manufacturing is at very high risk. Five of the eight largest healthcare security breaches since the beginning of 2010— those with more than one million records reportedly compromised—took place during the first six months of 2015. In fact, over 100 million healthcare records were reportedly compromised in 2015.2

Industrial networks top the list of systems most vulnerable to cybersecurity issues (McAfee)
IBM found that only 33% of manufacturers were performing penetration tests of their networks.

More than 1000 industrial automation and control systems (IACS) were targeted by the Dragonfly espionage malware program in 2014.

The number of attacks on industrial supervisory control and data acquisition (SCADA) systems doubled from 2013 to 2014.



Cc:
Subject: Suspension

Dear Client,

Generic non-personalized greeting

We have sent you this e-mail, because we have strong reason to belive, your account has been used by someone else.In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter. We've locked your Amazon account, and you have 36 hours to verify it, or we have the right to terminate it.

To confirm your identity with us click the link bellow:

https://www.amazon.com/exec/obidos/sign-in.html

Hovering over the link reveals it points to a non-Amazon site - "http://redirect.kereskedj.com"

Sincerely,

The Amazon Associates Team

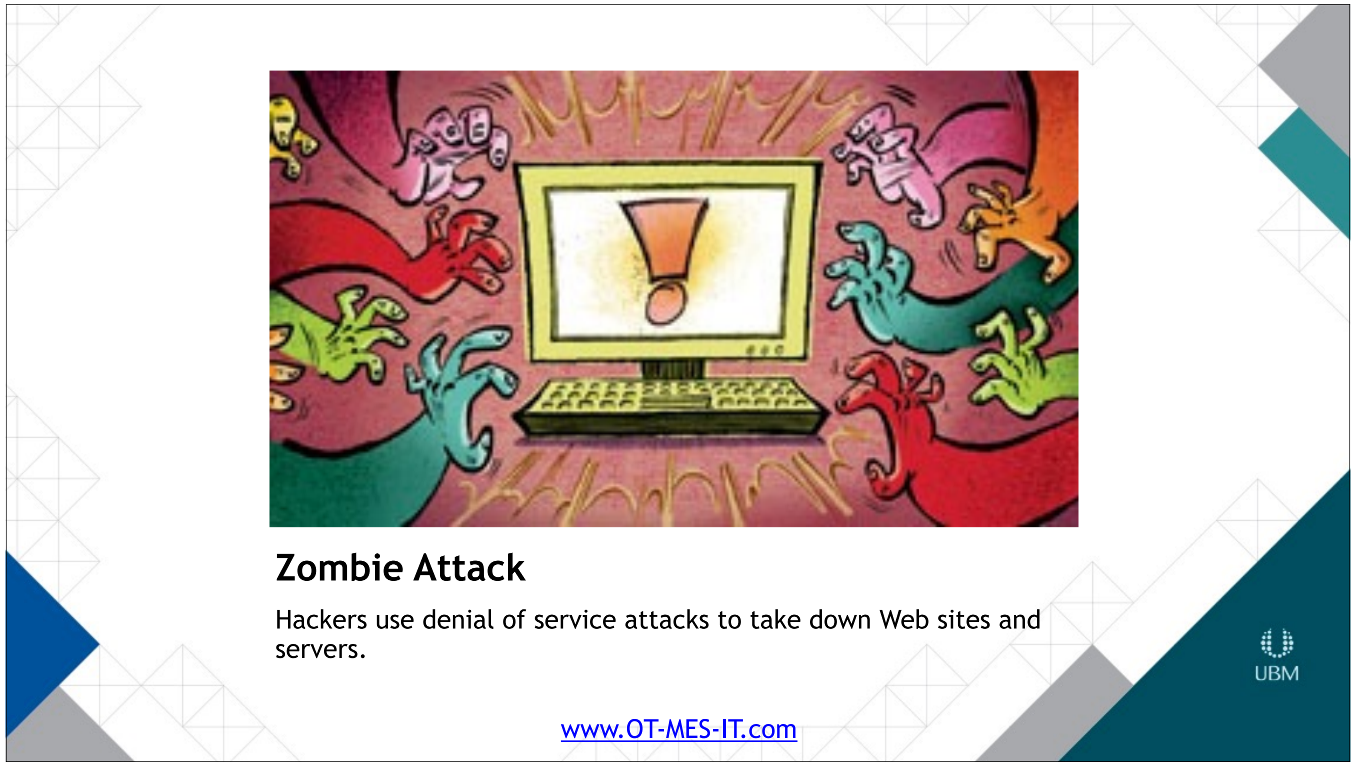
Phishing

Users on the network can let hackers in through emails.

Lee’s email: Sources of data compromise

60% of all attackers are “insiders” - 39% intentional, but 21% from good employees, contractors and consultants.

32% of attacks were by phishing and pharming.
http://www.darkreading.com/endpoint/91--of-cyberattacks-start-with-a-phishing-email/d/d-id/132770491% start with an email.



Zombie Attack

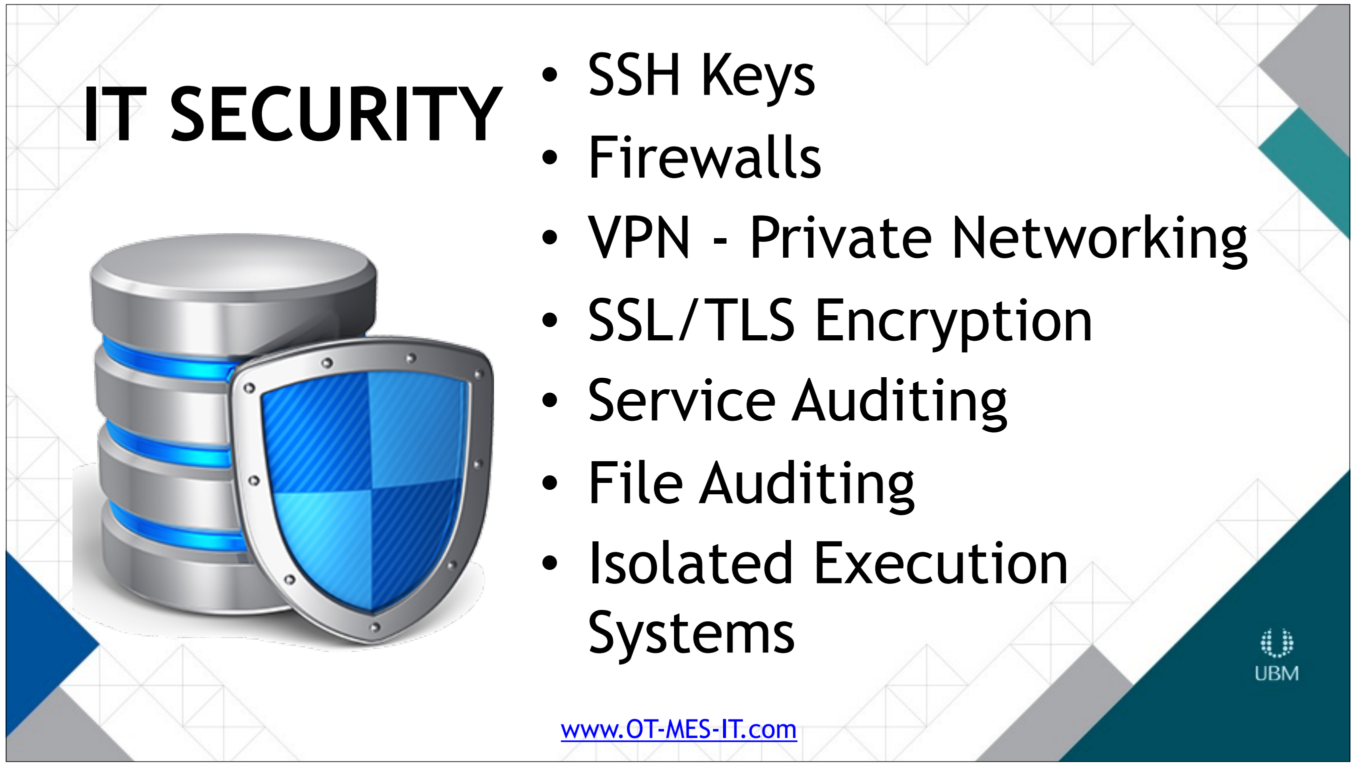
Hackers use denial of service attacks to take down Web sites and servers.

www.OT-MES-IT.com

HOW A "DENIAL OF SERVICE" ATTACK WORKS:

IN A TYPICAL CONNECTION, THE USER SENDS A MESSAGE ASKING THE SERVER TO AUTHENTICATE IT. THE SERVER RETURNS THE AUTHENTICATION APPROVAL TO THE USER. THE USER ACKNOWLEDGES THIS APPROVAL AND THEN IS ALLOWED ONTO THE SERVER.

IN A DENIAL OF SERVICE ATTACK, THE USER SENDS SEVERAL AUTHENTICATION REQUESTS TO THE SERVER, FILLING IT UP. ALL REQUESTS HAVE FALSE RETURN ADDRESSES, SO THE SERVER CAN'T FIND THE USER WHEN IT TRIES TO SEND THE AUTHENTICATION APPROVAL. THE SERVER WAITS, SOMETIMES MORE THAN A MINUTE, BEFORE CLOSING THE CONNECTION. WHEN IT DOES CLOSE THE CONNECTION, THE ATTACKER SENDS A NEW BATCH OF FORGED REQUESTS, AND THE PROCESS BEGINS AGAIN--TYING UP THE SERVICE INDEFINITELY.



IT SECURITY

- SSH Keys
- Firewalls
- VPN - Private Networking
- SSL/TLS Encryption
- Service Auditing
- File Auditing
- Isolated Execution Systems

www.OT-MES-IT.com

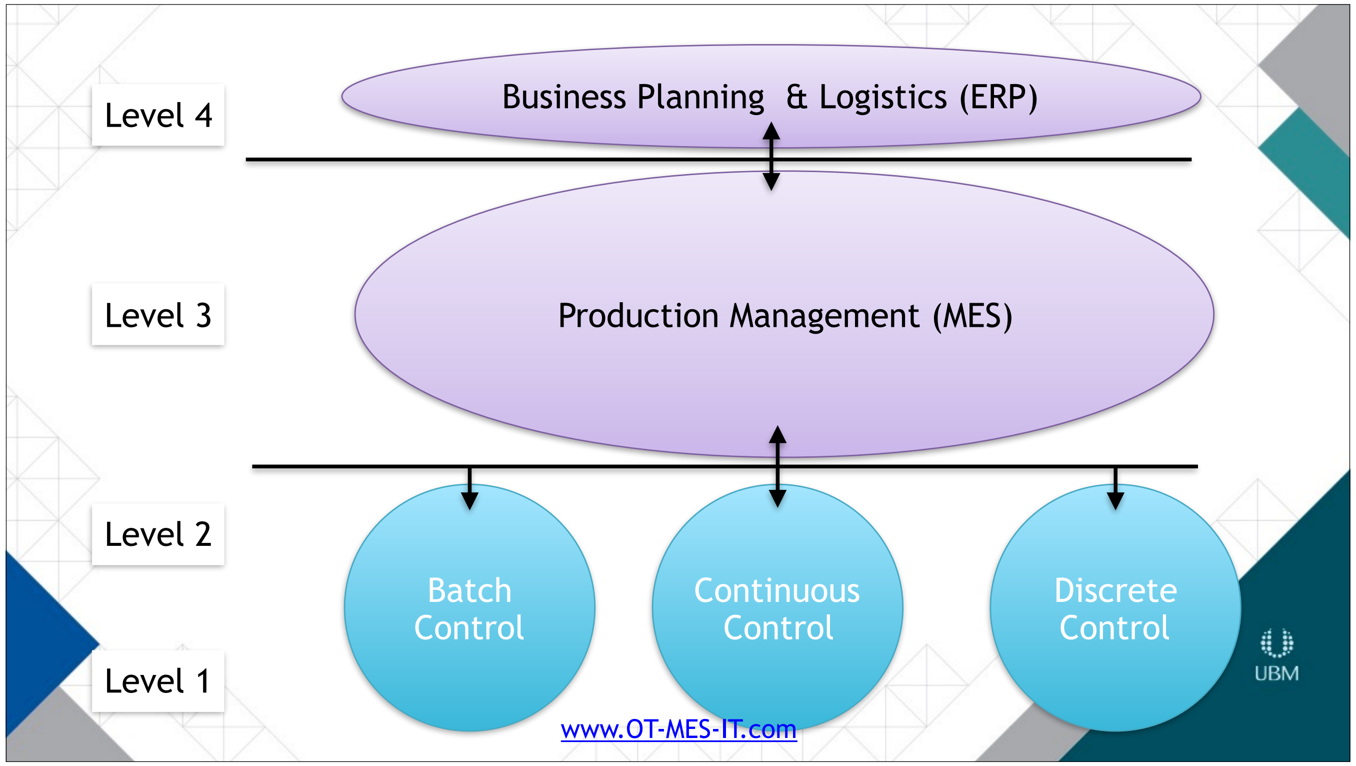
Bullet points for IT security measures from Digital Ocean tutorial: https://www.digitalocean.com/community/tutorials/7-security-measures-to-protect-your-servers

All of these can be implemented, but vulnerabilities aren’t just an IT problem when their network is converged with OT’s manufacturing network.

"If the stock exchange can be hacked, if the government of South Korea can be hacked and if the Department of Defense can be hacked--no company can be absolutely secure," Overly says. … "If your public-facing site is taken down, your business is going to stop," Zeller says.

As bad as it might be to deal with a downed Web site, in the worst case scenario the DDoS might be an early warning sign of a bigger attack or more serious data breach. During a DDoS, the hacker bombards the company's system with thousands upon thousands of useless pieces of information. In the midst of this, there's the potential for a hidden motive: that the hacker is trying to slip malicious code past digital security while the system is overwhelmed with extraneous data. Such malware could lead to a data breach and stolen confidential data. http://www.insidecounsel.com/2009/09/01/zombie-attack

Apologize for getting too networky and move on to how to exchange data with appliances, but make the point about **converging OT-IT networks being a mistake. Transition should be introducing how to keep them separate but exchange the data.**



www.OT-MES-IT.com

ISA levels for communication - the Production Management level (MES) is the link between the real-time oriented world of production automation and the central functions of the company represented by an enterprise resource planning system.

Who wants to own MES:
IT = security & .NET or C++
OT = availability & ladder logic or Modbus
Production Manager = don’t program, process responsibilities.

SMEs want data exchange without the infrastructure costs involved with IT’s security issues. But remember every PC-based solution on the factory floor opens their network along with the company’s trade secrets to vulnerabilities and threats.

Lee’s email: Indiscriminate internetworking is the biggest problem facing manufacturing today. The problem is that every message might be an attack, whether plain text or encrypted, and the consequences of attacks on manufacturing networks are unacceptable. An attack which alters recipes can make people sick. Compromise of a CNC mill, robot, or inspection system which can produce defective components, which result in massive recalls. Unlike an IT system, we cannot just "restore from backup".

Windows Vulnerabilities

Using appliances with Linux embedded removes IT issues from the data exchange between OT and IT

www.OT-MES-IT.com

“Traditionally, software applications run on top of a general-purpose operating system, which uses the hardware resources of the computer (primarily memory, disk storage, processing power, and networking bandwidth) to meet the computing needs of the user. The main issue with the traditional model is related to complexity.” Leaves security vulnerabilities because common applications are always running and are accessible.

“A computer appliance is a specialized computing device with special hardware and/or firmware built to serve a particular need or function. Computer appliances differ from general-purpose computers such as a desktop computer or server in that they are usually not designed to be modified by the end user. All functionality is 'sealed in' at the factory.”

“closed architecture”

A point to make about Stuxnet attack on Siemens PLCs and the BlackPOS attack on the NCR cash registers at Target is that, because they were so specific to these devices, the firewalls and virus software did not have any patterns in their libraries to match up and catch them. McAfee, Symantec, Microsoft and others were using a Black Hat defense looking for Windows 7 attacks, which let these malwares through. One looked like a file of strings, which it was, and the other was aimed at XP, which was no longer supported by Microsoft and had no security updates for the previous two years. The Target malware was planted by an attack on their web server, then worked its way to the cash registers, welcomed in by the firewalls.

APPLIANCE

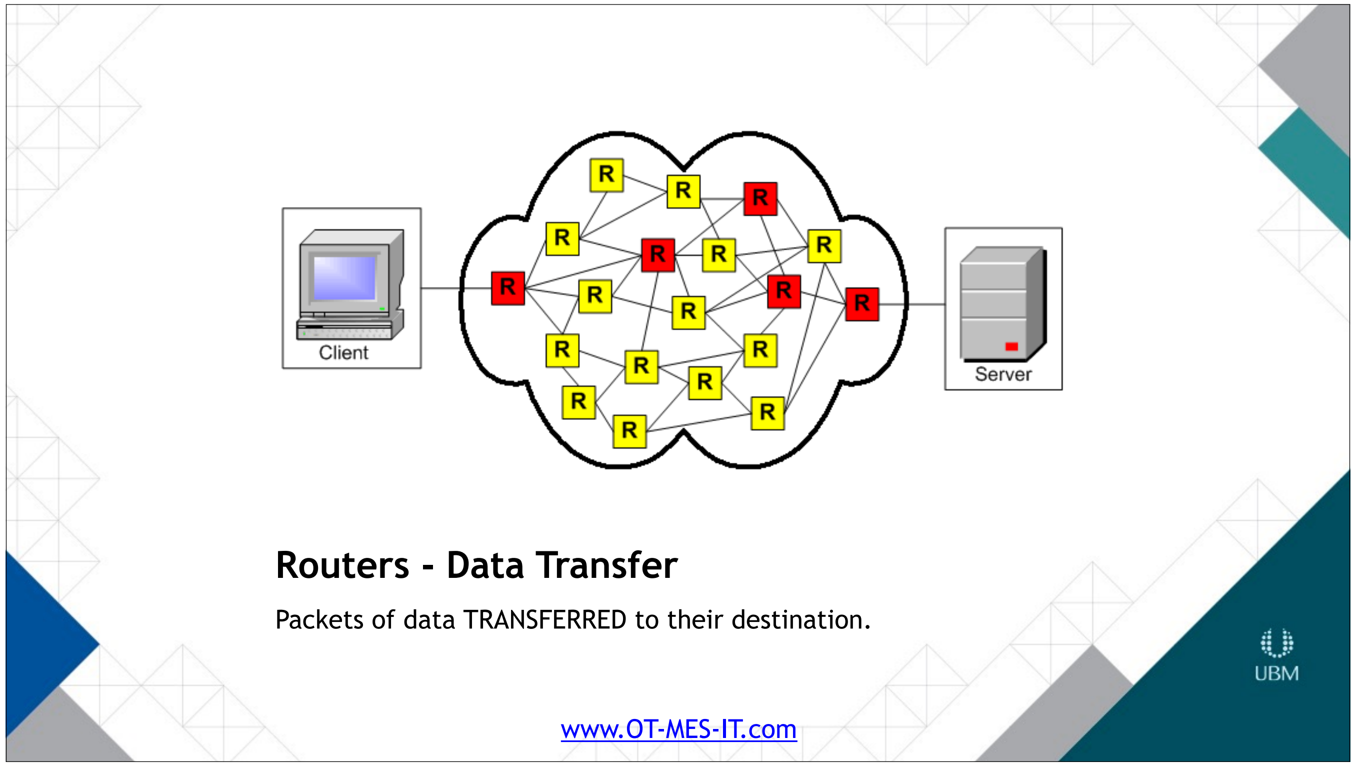
Embedded “computer”
with one task

www.OT-MES-IT.com

Modem = Internet Gateway Appliance
Gas pump = embedded “computer”
OT-IT translation = MES gateway appliance.

Pros:
…no specialized knowledge is required, and that the desired functionality will instantly be available, quickly and easily at a low cost, saving businesses and end users time and effort. The device is as easy to use as a kitchen toaster.

Flash Memory
Processor or Application-Specific Integrated Chip(s (ASICs)
RAM
Separate Ethernet Network ports
Linux-based operating system or micro-kernel



Routers - Data Transfer

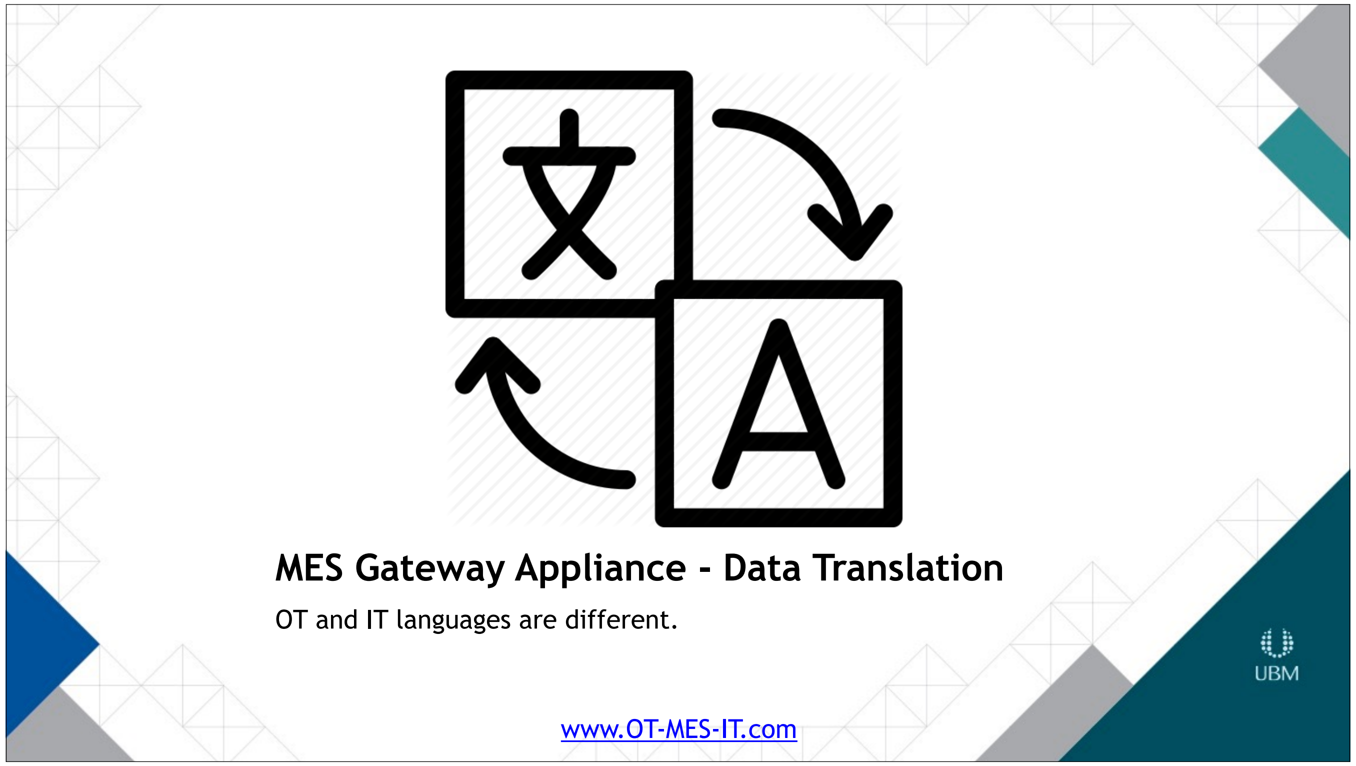
Packets of data TRANSFERRED to their destination.

www.OT-MES-IT.com

Remember the data types of IT: confidential — servers, users, and locations (IP addresses) of devices need to be hidden.

Costly to hide from outside world because the vulnerability is built in to the OS, network links, and bad habits e.g. DMZs, white hat firewalls, double authentication to increase security.

Security: IT is used to handling router issues, but what about SME operations who cannot incur IT infrastructure costs?



MES Gateway Appliance - Data Translation

OT and IT languages are different.

www.OT-MES-IT.com

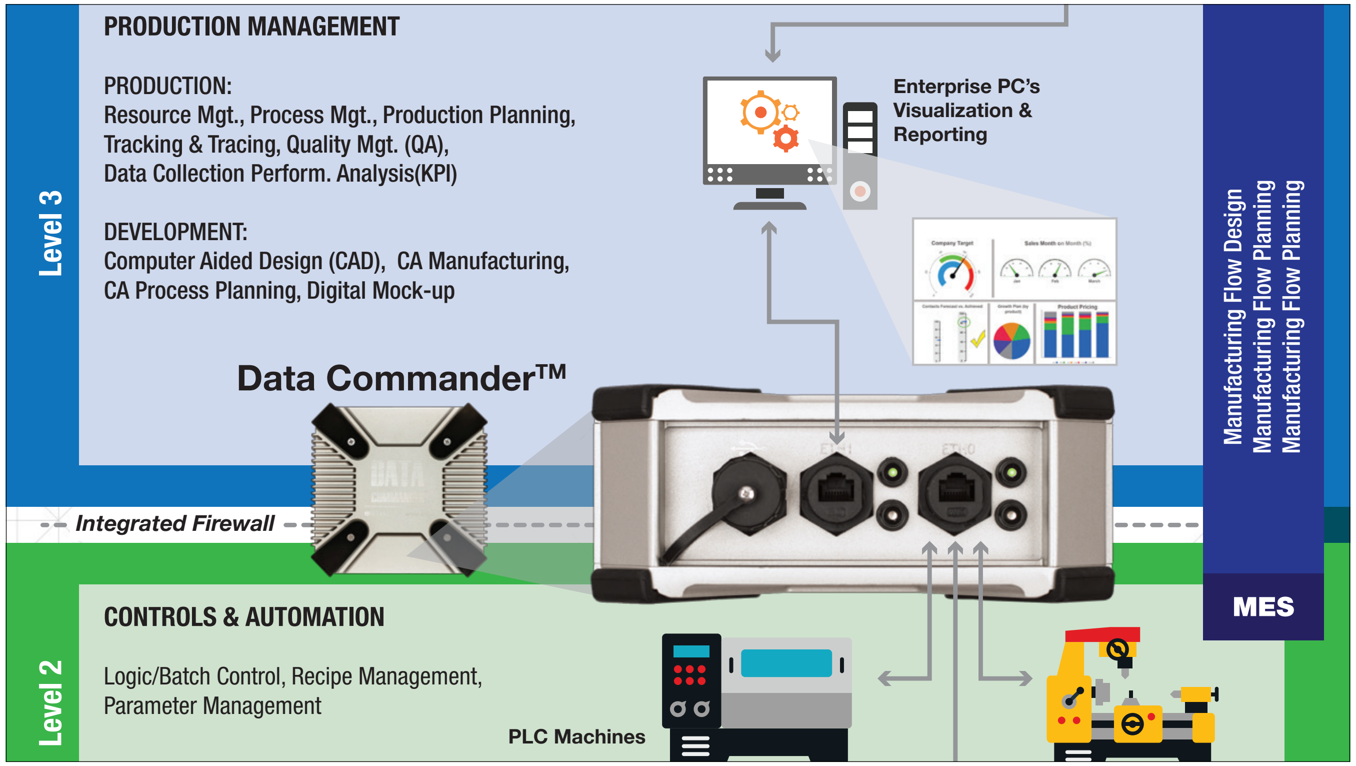
Factory (OT) data types vs IT data types:
Up until now we’ve talked from the IT perspective about the differences between an appliance and a computer and how an appliance’s embedded firmware hides its application, but what about OT’s concern for their data types?

OT’s security solution lies in the application of the appliance. Several features of an MES Gateway Appliance contribute to the concept of end-to-end security between OT and IT. The proprietary language that lies within the appliance TRANSLATES vs TRANSFERS (e.g. router) data.

Remember that OT data types are different than IT. Field mapping between the languages and networks not only eliminates programming via point-and-click drop-down menus, but it also prevents malware from traveling across the appliance from the OT network to the IT network and vice versa. The reason lies in the nature of malware attacks and the natural differences between the languages used in IT and OT networks.

For example, if a virus somehow goes beyond the protections that are inherent in the design of appliances, because of the embedded application (firmware), the hack still doesn’t know what the proprietary application is (unlike a common OS), and even if they somehow figure out the location, and then further figure out what the application is, the hack is captive inside the application because whatever IT language got them this far dies within the appliance because on the OT side, there is a totally different language being spoken to the OT devices.

Security: Lee’s cargo ship example.



Level 3

PRODUCTION MANAGEMENT

PRODUCTION:
Resource Mgt., Process Mgt., Production Planning,
Tracking & Tracing, Quality Mgt. (QA),
Data Collection Perform. Analysis(KPI)

DEVELOPMENT:
Computer Aided Design (CAD), CA Manufacturing,
CA Process Planning, Digital Mock-up

Enterprise PC's
Visualization &
Reporting

Data Commander™

Integrated Firewall

Manufacturing Flow Design
Manufacturing Flow Planning
Manufacturing Flow Planning

MES

Level 2

CONTROLS & AUTOMATION

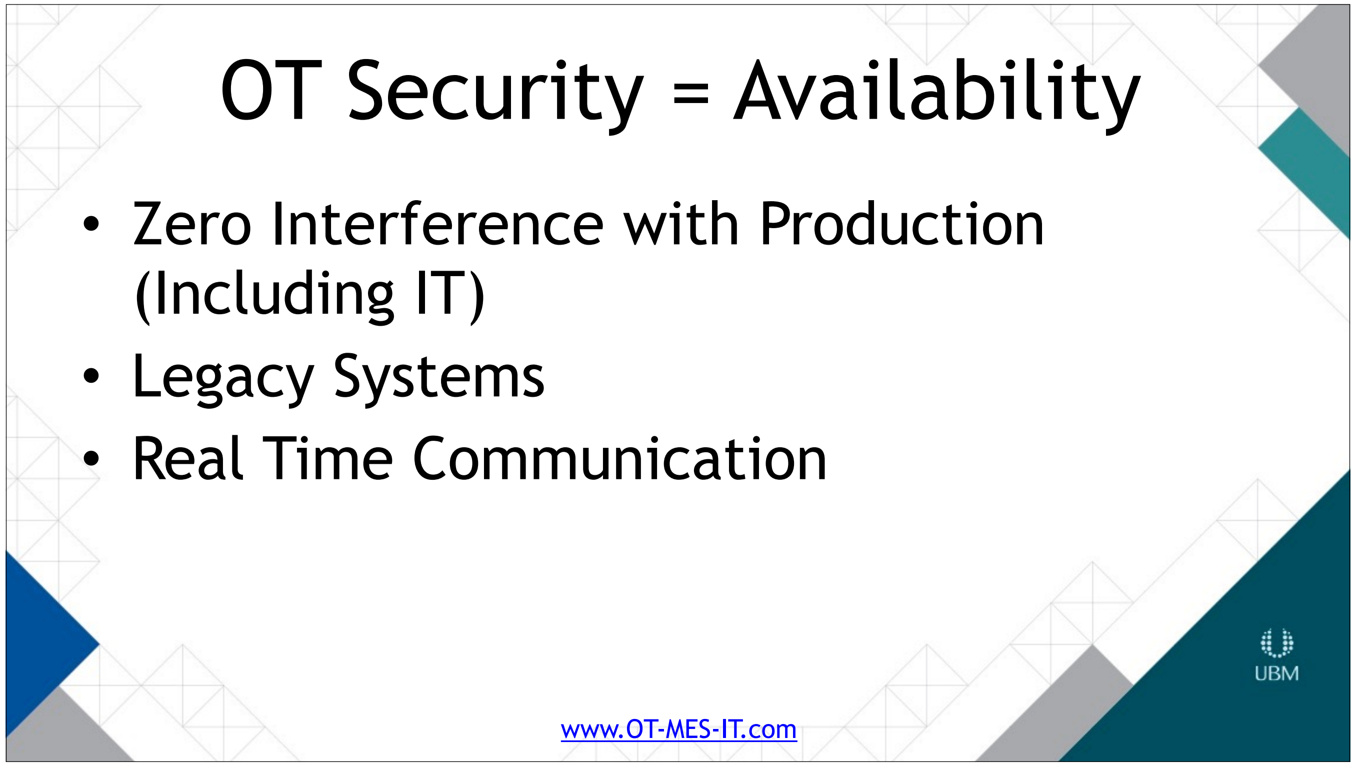
Logic/Batch Control, Recipe Management,
Parameter Management

PLC Machines

Rather than packets of data being able to go from one network to another like a router, an appliance running a single proprietary application like an MES Gateway Appliance doesn't pass data through unless the fields are mapped between the two networks using the custom application.

In this diagram, we're showing where our MES Gateway Appliance sits between OT and IT networks. Notice the two different physical ethernet NIC ports. Not only are the OT and IT networks separated by languages in the application, but the two networks are physically different from each other and cannot be bridged via software unlike in Windows firewall properties that can be manipulated by hackers.

Up until now, only IT's security perspectives have been addressed. Using an appliance does make it easier for Production Management to begin Smart Manufacturing efforts in earnest, but what about OT's security concerns. The subject is end-to-end security after all, and not IIoT security for the IT department.



OT Security = Availability

- Zero Interference with Production (Including IT)
- Legacy Systems
- Real Time Communication

www.OT-MES-IT.com

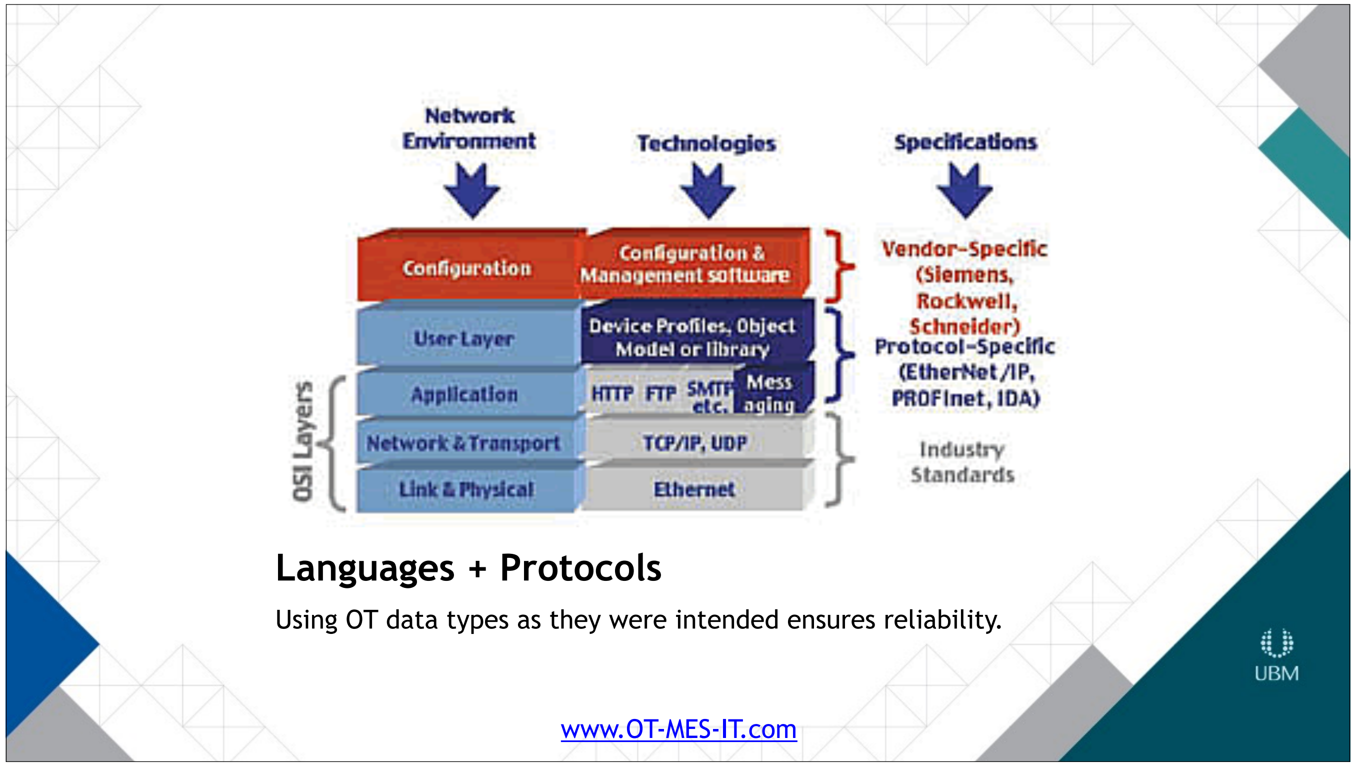
A secure production line means quite a different thing from OT's perspective than IT's protectiveness. We've covered how viruses and malware don't travel through an MES Gateway Appliance, but what does that mean for production?

The application on the appliance speaks the native languages of the devices and communicates directly with them - similar to the older practice of station addresses before the advent of ethernet communication on the factory floor.

-That means OT is able to operate their machines' systems~~, that are instrumentation based rather than C++ or .Net based,~~ without having to interrupt production for IT security updates to PCs or have to maintain middleware on the factory floor.

-That means OT doesn't have to change dated but functional legacy systems. Instead of redesigning PLCs and other devices to use OPC or OPC UA, current devices can communicate in their native language because the appliance is safely translating it into IT's language for the other network.

-And that means that the nature of OT's data doesn't have to compete with the nature of IT's data. OT's data is in small packets and is meant to keep up with the real time world of manufacturing's EVENT BASED data as opposed to the POLLING nature of large IT packets used by OPC for example.



Languages + Protocols

Using OT data types as they were intended ensures reliability.

www.OT-MES-IT.com

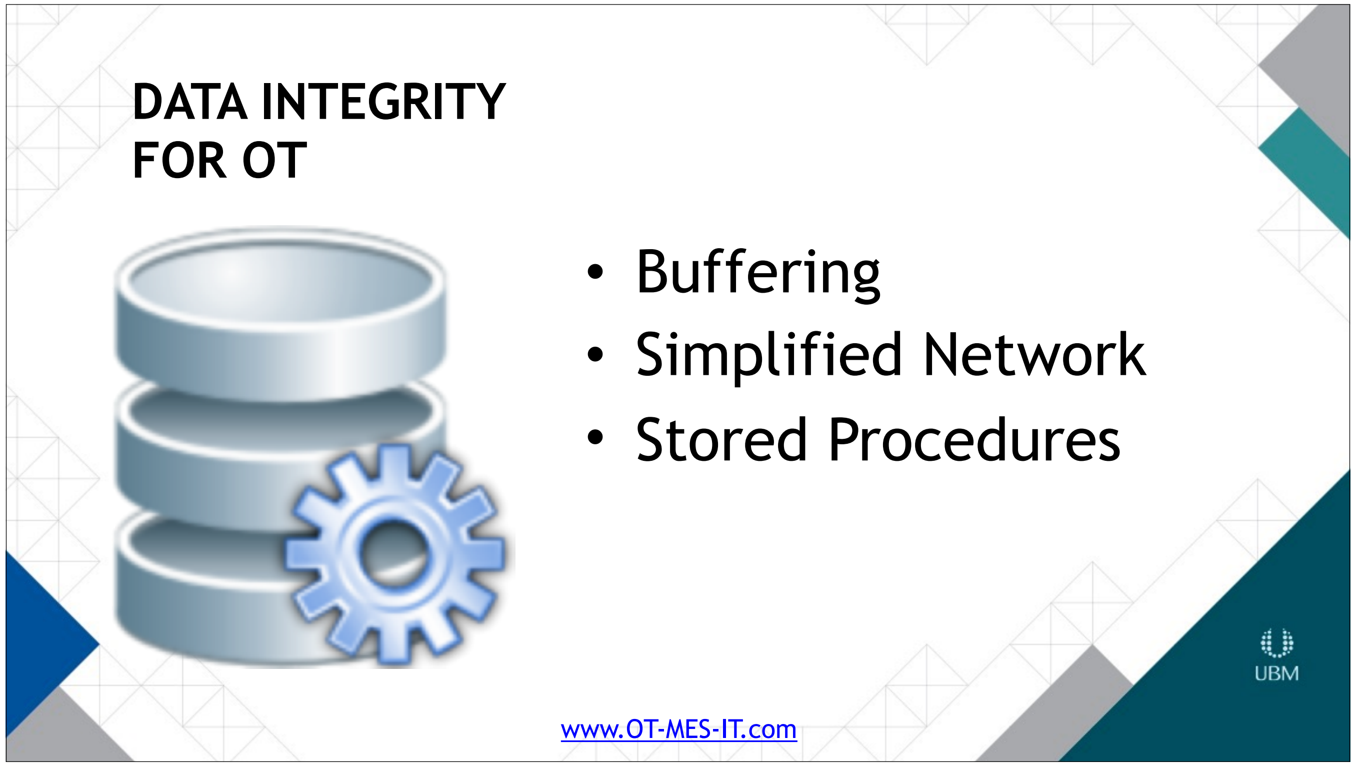
The purpose of this table is not to try to make network experts out of anyone. The purpose of this table is to show the two considerations inherent in reliable communication on a machine network.

LANGUAGE:
An MES Gateway Appliance can speak in the native language of the devices. The interface of the appliance communicates in whatever language the devices' were manufactured with. Communication isn't limited in any way because the appliance and the device is speaking in the exact same language. For an alternative example, OPC (UA) has to be added to a device for it to communicate with an OPC server and may not include all of the memory areas of a PLC, and then once the machine communication is merged to the network, IT has to write an application to work with the PLC data hosted on the OPC server.

PROTOCOLS:
An MES Gateway Appliance also uses reliable Network Transports. Some protocols are proprietary for machine communication (e.g. DeviceNet, ProfiNet, or Ethernet/IP) and others are standard like UDP (real-time I/O control), but what's important to understand about industrial protocols is that they don't have the same overhead as IT network infrastructure because the network is not broadcasting when an MES Gateway Appliance is being used.

Because the appliance application TRANSLATES data rather than TRANSFERS data across the OT and IT networks, the factory can design their Industrial Ethernet to suit their OT needs for real-time data secure in the knowledge that the event-based bits of information are communicating natively and across the protocols they were intended to.

In the past before MES Gateway Appliances were available for OT, the Industrial Ethernet would mirror the IT infrastructure bringing with it latency issues, packet loss under congestion, and network security issues that interfere with the reliability of machine communication and hence machine availability.

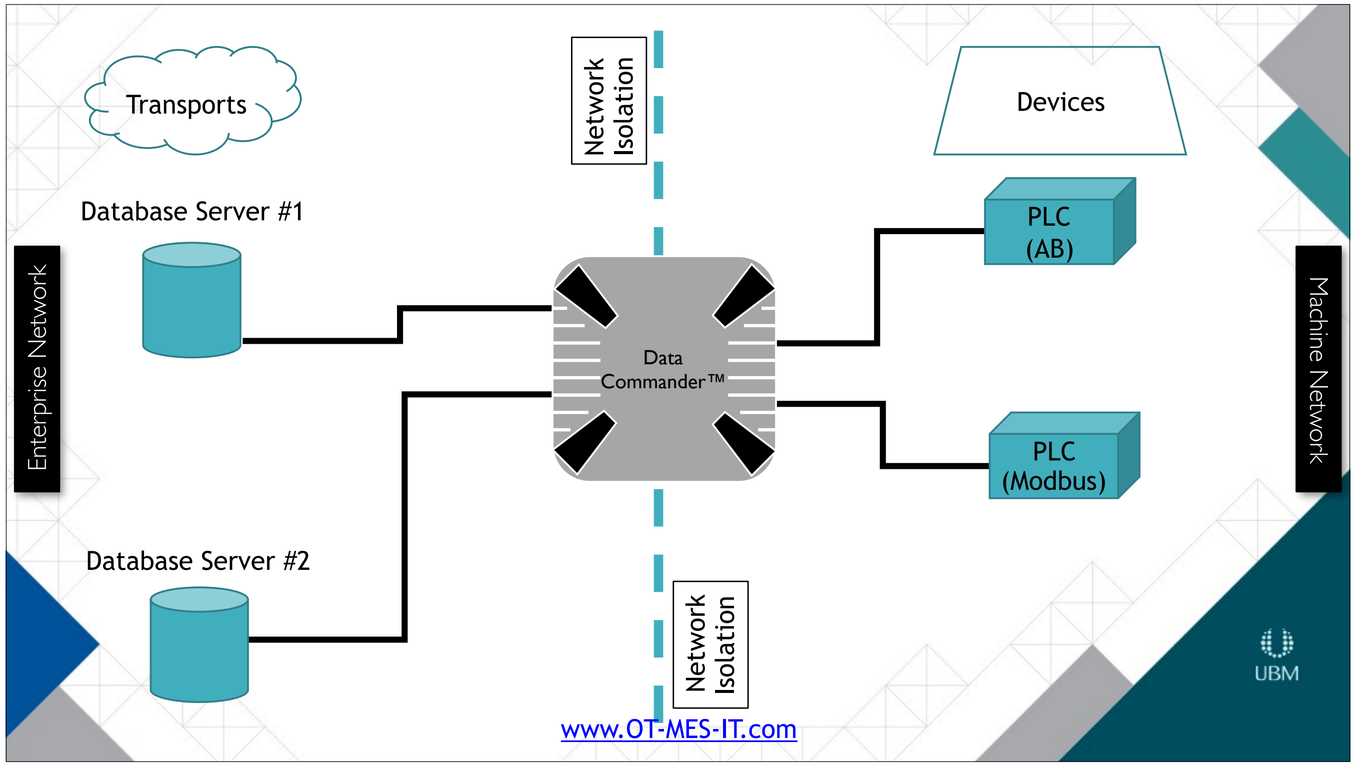


DATA INTEGRITY FOR OT

- Buffering
- Simplified Network
- Stored Procedures

www.OT-MES-IT.com

And the final security feature of an MES Gateway Appliance is the quality of the data itself.
The Store and Forward feature of the application “buffers” data so none is lost in case of network interruptions.
Data from multiple places can be combined in the appliance’s application to do calculations or stacking IP addresses - further offloading any possible network interference with the machines and simplifying network infrastructure.
Use of Stored Procedures filter raw data from being inserted directly into IT’s database or OT’s machines avoiding garbage in/garbage out scenarios.



Another feature / benefit is that by converting the data, doing calculations, and delivering the data to the database via calls to its stored procedures is that IT and the DBAs control the insertion and extraction of data, and we replace the need for PC-based applications to process the raw data from the devices, or convert strictly formatted EDI messages into database record formats and data type.

The MES Gateway Appliance not only protects the confidentiality of the IT network, but simplifies the network requirements on the OT network to ensure machine availability.

Gutmenge (pcs) 8324634

Produktion (h) 6090

Ausschuss (pcs) 114293

Stillstand (h) 555

www.OT-MES-IT.com

Summarize roles and the issue of ownership in terms of security.
-Production Management wants reliable data exchange, without being dependent on specialized programming
-IT has to protect the entire enterprise from cyber attacks.
-and OT has to ensure that continuous operation is maintained.

IIoT and Smart Manufacturing pitfalls can be avoided by looking beyond the 30,000 foot fly-over marketing. Smart Manufacturing deployment can be simplified and more secure by respecting the responsibilities of production's engineers and IT professionals by isolating, rather than converging, OT and IT networks with an MES Gateway Appliance instead of PC based solutions and OPC middleware.