The Two Things You Need To Know

Dave Edstrom
CTO Memex
Former President
Chairman and President MTConnect Institute
MEMEX PROVEN SINCE 1992

Leading the Industry – Building on Key Trends

- Co-developed bubble memory replacement for Fanuc 6/9/11/12
- Created Fanuc 0 & 10 memory upgrades
- Released the Mx1000 BTR
- Created Network Connections to Fanuc
- FMS projects

1999-2007 Network Connectivity
- First CNC Web connection
- Became largest DNC vendor in North America
- Launched Mx1000 Universal Machine Tool Interface

2008-2011 Industry Standards
- Joins MTConnect Technical Advisory Group
- Launches MERLIN OEE + DNC and gains key customers
- Asked to co-chair MTConnect Legacy Machine Tool Working Group

2012-2013 Machine Connections
- Selected by Microsoft as MES
- Commercialization Phase
- MERLIN earns Frost & Sullivan Innovation Award

2014-2016 Software
- Mazak selects MERLIN for Kentucky plant roll-out
- MEMEX becomes public company under the call letters “OEE”
- Cisco and Mazak select MERLIN for SmartBOX

Are you ready for the next industrial revolution?
1. How do we connect our most important assets (machine tools, systems, operators, sensors, ....)

2. How do we **safely** and **securely** connect these countless IIoT assets to each other and to the outside world along with countless other systems?

   * Create silos of information?

Deciding to NOT digitize your plant is a decision to go out of business.

**Digitize or PERISH!**

Photos owned by Dave Edstrom
Different Devices, Common Connection

For more info ➔ http://MemexOEE.com/MTConnect

Adapter (hw and/or SW)

Simple Hierarchical Data Representation Format
-- Pipe delimited ASCII data
Streaming to the agent (only send data when it changes) -- (not part of official MTConnect spec)
2015-09-29T23:59:33.460470Z
|htemp|
WARNING|HTEMP|1|HIGH|Oil Temperature High

Agent

Agent receives simple Commands from clients and returns XML back.
Agent simply looks like a Website to the Outside world
Agent maps SHDR from Adapter to XML by using agent.cfg, Devices.xml, Schema Definition Files (.xsd)
Stores info in circular buffer

Software today can easily speak HTTP and XML.
MTConnect provides simple discovery mechanism such as probe.
Easy data access by current, sample and asset.
The client sends these commands to the agent

Apps

Client Application (shop floor monitoring Such as MERLIN)
What Is Cyber-Physical Security (CPS)?

* Cyber-Physical Systems control physical devices and are monitored/controlled by a computer and the term was coined by Helen Gill at the National Science Foundation in the 2006 timeframe.

* Cyber-Physical Security (according to IEEE): “In contrast to cyber security, the goal of cyber-physical security is to protect the whole cyber-physical system, which uses widespread sensing, communication and control to operate safely and reliably.”

* In manufacturing, CPS means protecting machine tools, operators, sensors and anything that can “do something physical” in your shops and plants.
**What Are Examples of CPS Breaches?**

- **Stuxnet** – Most famous example of a CPS attack
  - Iranian centrifuges spin out of control, but report all is well.
  - Siemens S7 controller still had the default login/password
- **MEDJACK** – Hijacking Medical Devices
  - “This includes diagnostic equipment (PET scanners, CT scanners, MRI machines, etc.), therapeutic equipment (infusion pumps, medical lasers and LASIK surgical machines), and life support equipment (heart-lung machines, medical ventilators, extracorporeal membrane oxygenation machines and dialysis machines) and much more.” – ComputerWorld article by Darlene Storm on MEDJACK and TrapX
- **Many of these IoT/IIoT devices were NEVER designed to be secure!**
  - **Tire Pressure Monitoring System Attack (TPMS)** - unencrypted
    - 100 zero PSI per second on each tire
  - **Remote Hack of Jeep**
    - Jeep remotely hacked – Fiat Chrysler recalls 1.4 million cars
    - 60 Minutes Lesley Stahl

Photos licensed under the Creative Commons Attribution-Share Alike 3.0 Unported license.
Which is your shop or plant’s security model?

Think of security in the same way that the United States Secret Service protects the President – in layers upon layers of security with clear plans on how to deal with breaches at each level.

Authentication – who or what are you?

Authorization – what are you or the device allowed to do?

We all know what IT (Informational Technology) is, but what is **Operational technology (OT)**?

* OT is hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices

Protect (encrypting) data in-flight (on a network) and at rest (sitting on a disk drive)
Security Principles – The Basics

Confidentiality (WHO or WHAT is ALLOWED see this?)

Operational Uptime & Secure Availability of Services

+ Authenticity (How do I KNOW who you REALLY are?)

Integrity (HOW do I KNOW this has NOT been tampered with?)
The Two Things You Need To Know

Presentation by Dave Edstrom, CTO for Memex  -- McMaster Manufacturing Forum 2016

- At first blush, why not create a back door for the FBI?
- No matter what it is called, a backdoor is a backdoor is a backdoor
- IF Apple is (eventually) forced to create a backdoor, then other companies will be forced to create back doors as well and then the bad guys will quickly figure out how to use the back doors and your information will be at risk – your financial, your personal information, your medical information, ….
- Even if Apple later agrees, the bad guys will use encryption communication anyway as bad guys don't follow laws
- This is like trying to outlaw math – BIG surprise that United States politicians DON'T get it
- The outcome of this will have a HUGE affect in ALL on American’s personal and professional lives
- General Michael Hayden (only person to be Director of BOTH NSA & CIA) agrees with Apple

The FBI flag is in the public domain because it was published in the United States between 1923 and 1977 and without a copyright notice.

Apple store photo - Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
Industry Call to Action

• The “Orange Book” was the bible for computer system security in the 80s, 90s and early 2000s
  • A — Verified protection
  • B — Mandatory protection
  • C — Discretionary protection
  • D — Minimal protection

• The industry needs a Manufacturing Trusted Plant Evaluation Criteria Standard
Thanks!

Dave Edstrom
CTO Memex
Former President
Chairman and President MTConnect Institute