OT versus IT

© *Rob Hulsebos*

Version 12-Feb-2024

Introduction

Whenever I talk to companies and people active in the industrial cybersecurity industry, it is always mentioned that "OT" (Operations Technology) is different from "IT" (Information Technology) – with respect to equipment, software, work procedures and people.

But what *is* OT? Gardner says:

> *The hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise.*

Some companies put IT and OT staff in one department, but it wouldn't surprise me if such a department consists of two teams – one team doing the IT-work and the other team doing the OT-work. There are special courses for IT people, learning them what OT is, trying to bring more understanding[1].

But what *are* the differences? Let's look at it in more detail below. It is not only about cybersecurity aspects, but also about infrastructure, protocols and software.

> *Note: the differences between IT and OT are described very general. It does not mean that every IT-department is like described here, just like there will be OT-departments that in no way resemble the description below. Your mileage may vary!*

1 Procedures

Focus

(IT) The focus is on informational activities.

(OT) The focus is on production (goods, gas, electricity, transportation, etc.)

[1] *I've heard of cases where IT-engineers didn't want to work with OT equipment running on Windows NT (which may be older than the engineer itself). Why work on "Outdated Technology" if there is newer and sexier technology like Win11, cloud and AI ?*

CIA or AIC

The letters A,I,C stand for Confidentiality, Integrity and Availability. The sequence CIA or AIC indicates the priority of these aspects.

(IT) Uses CIA: the "Confidentiality" of data is most important (often enforced by privacy laws).

(OT) Uses AIC: the "Availability" of the system is the most important: the production must run 24/7, or systems must be available 24/7.

Safety

(IT) Standard (consumer) product *safety* applies to IT products. There is no relation to cybersecurity.

(OT) The safety aspects of a machine, production line or industrial installation are very important, perhaps even more important than the AIC aspects, summarized as "SAIC".

Example: a problem with the safety in a chemical plant may cause massive damage and/or deaths (for example, see https://www.youtube.com/watch?v=_KuGizBjDXo). To guard safety, special "Safety PLC's" can be used, or "Safety Instrument Systems" (SIS). Hacks in a safety PLC / SIS can be very dangerous, i.e. what happened in Saudi Arabia in 2017? (the "Triconex" hack which fortunately didn't do any damage).

Cybersecurity responsibility

(IT) The IT department.

(OT) Usually the production department, sometimes a separate department.

Working hours

(IT) 8-8, on weekdays

(OT) 24 hours / 365 days per year

Security awareness

(IT) High (but not always high enough)

(OT) Low (but is increasing)

Standards

(IT) ISO 27000 series.

(OT) IEC 62443, NIST 800, many other standards per type of industry.

Consequences of a hack

(IT) A successful hack may stop an IT-system, erase its data, but not destroy it physically or its environment.

(OT) A successful hack may physically destroy an industrial system and/or cause widespread damage to its environment.

2 Equipment

Access to equipment

(IT) Network infrastructure equipment is mounted in cabinets, often in locked and conditioned rooms.

(OT) Network infrastructure equipment is often mounted in machines itself, or along a production line. This is the reason that there are many switches on the market with a small number of Ethernet ports (say: 4 or 8) as this is sufficient for the equipment in the immediate vicinity.

Environment

(IT) Usually found in normal climatic conditions.

(OT) Often found in environmentally unfriendly environments (temperature, vibration, humidity, dust, EMC, etc.)

Figure: OT switch being used in environment with lot of dust

Managed / unmanaged switches

(IT) Managed switches are used everywhere.

(OT) It is still very common to find unmanaged switches. The reason is the price difference with managed switches.

Size of switches

(IT) Switches have as much ports (32, 48, …) as possible, to accommodate many desktop PC's, printers and other equipment.

(OT) Switches often have only 4 or 8 ports, especially on production locations. Switches with more ports are used at the higher levels of a production system. It is also common to see devices with a built-in switch function with only 2 ports, allowing for easy 'daisy-chaining' which is very useful

along a production line or in a cabinet. It is also common to have devices with 2 Ethernet ports internally being a 3-port switch (the 3rd port used internally).

Lifespan of equipment

(IT) Lifetime of equipment is typically short, i.e. 3..5 years.

(OT) Lifetime of equipment can be 10..20 years. Manufacturers are often able to support this period with spare parts. Backwards compatibility is important in case a product is taken off the market and replaced by a newer version.

Ethernet connector

(IT) Always RJ45.

(OT) More than 20 different Ethernet connectors may be found, depending on the industry branch and preferences of some vendors. The reason for this diversity is that connectors must be able to function well in humid / wet environments, in temperature ranges of -40..+80C, be able to withstand vibration, carry extra power supply signals, etc. Popular is the M12-D connector.

Figure: an M12-D Ethernet connector

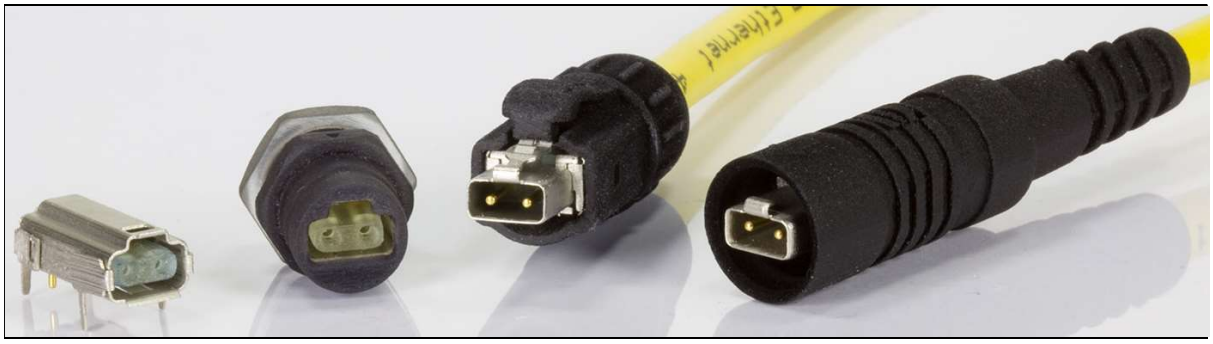


Figure: the new "Single Pair Ethernet" (SPE) connector (source: Harting)

Ethernet speed

(IT) Usually all equipment uses Ethernet, the faster the better (minimum 1 Gbit/s). Networks running at 100 Mbit/s are scarce and those at 10 Mbit/s virtually nonexistent. The same holds for WiFi: the faster the better, meaning: using a recent version such as 802.11ac and better.

(OT) When Ethernet is used for control purposes, do not be surprised if it is running at 100 Mbit/s. This is a very high speed for a control network, especially when dedicated industrial protocols are used (see below).

Ethernet wiring

(IT) Star-based at the lowest level, perhaps with mesh at higher levels (for redundancy).

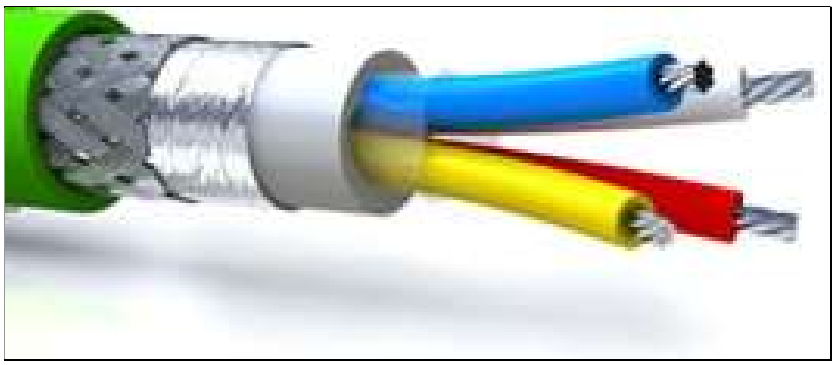
(OT) Usually these networks are also star-based, but as this may cost a lot of cable in control cabinets, conveyor belts or long machines, some industrial Ethernet protocols allow daisy-chained wiring. No switch is needed for this. This way of wiring is do different from the usual Ethernet way of wiring that sometimes it isn't recognized as being Ethernet.

A daisy-chained industrial Ethernet (Sercos).

Ethernet cabling

(IT) Standard CAT5e, CAT6 or higher. Even when networks are running at 100 Mbit/s, cables always have 4 pairs, even though half of them are not used. Shielded cable is not needed in many cases.

(OT) At the control level often 100 Mbit/s is used, and 2-pair cables are common because it is sufficient for running at this speed. Using shielded cable is common practice. The colors of the wires may differ from what is usual in Ethernet; some might not even recognize it as being Ethernet. One vendor calls their cable "ITP" – Industrial Twisted Pair.



A "ProfiNet" industrial Ethernet cable (note the 4 wires,
the different color scheme, and the shielding).

Protocols

(IT) The TCP/IP family will be used. Many vendor-specific protocol exists.

(OT) There is an enormous diversity in protocols, which even differs per branch of industry. For example, protocols used in machine building (and their vendors!) are likely to be ProfiNet, Ethercat, Ethernet/IP, Modbus/TCP (and many more) but in building automation one will find BacNet/IP (and many more), in process automation VNet/IP (and many more), and in airplanes, ships, trains, etc. yet others.

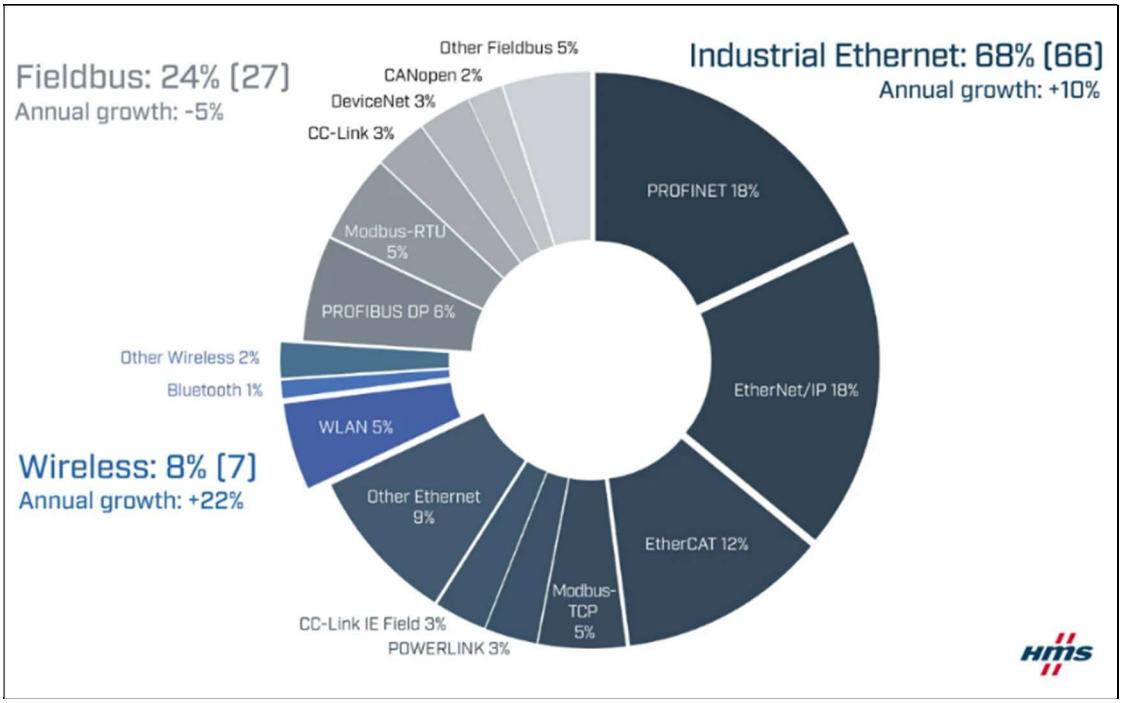


Figure: Market share of OT protocols (source: HMS)

These protocols are all found in products of the vendors that operate in those markets only, i.e. it is impossible (or very difficult) to use a protocol which is not common in such a market. Many protocols have no publicly available specification.

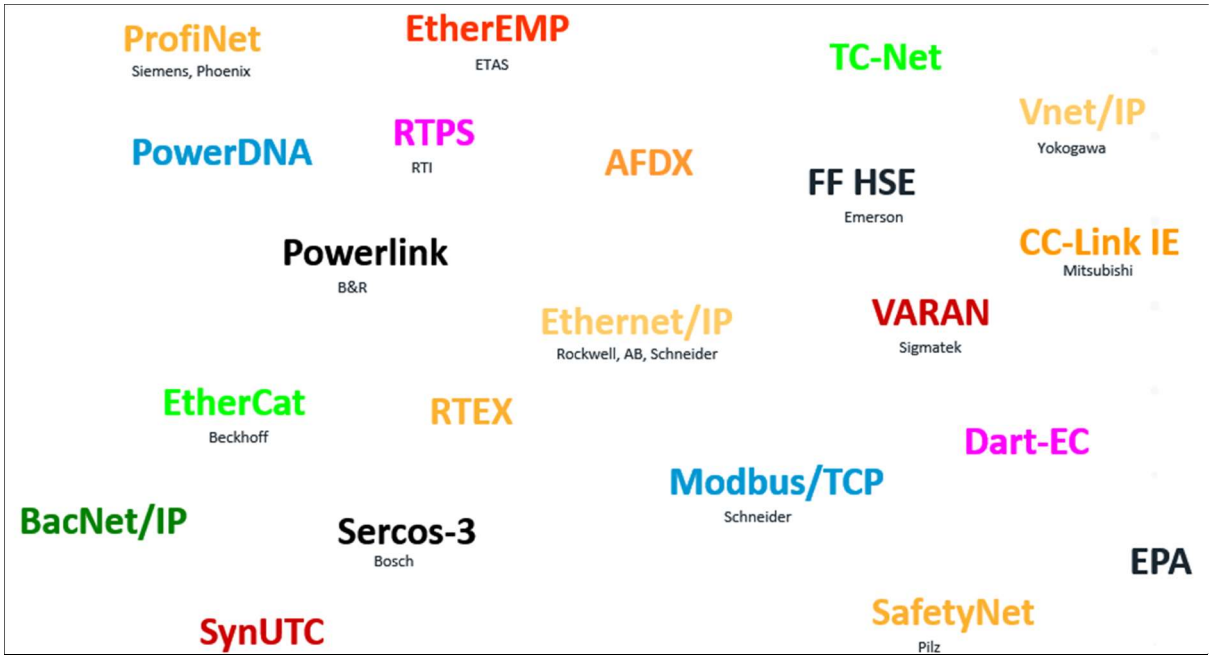


Figure: an overview of popular industrial Ethernet protocols.

IP-addressing

(IT) IP-addresses are usually dynamically assigned, via DHCP.

(OT) IP-addresses are often statically set, because the IP-address is related to the function/role that each device has.

Bandwidth

(IT) The more the better (Gbit/s).

(OT) Many industrial protocols run at speeds of 100 Mbit/s. Although it doesn't look much, it is still an enormous bandwidth given the fact that OT-devices often send only very small amounts of data. Nevertheless, there is a trend to move to higher speeds.

Packet size

(IT) Generally, packets contain a lot of data. The packet headers are generally large (many bytes), but this must be seen in relation to the amount of data.

(OT) Many protocols are used for transferring I/O (input/output) data, usually only a few bytes, so packet sizes are generally very small. Protocols are optimized to have a small as possible packet header.

Type of network traffic

(IT) Websites, database access, file access, voice, video, bulk data, etc.

(OT) Input/output, sensors, monitoring, supervisory control, etc.

Network load

(IT) Highly variable

(OT) Can be very constant, as protocols run cyclically, with always the same devices and with the same amount of data.

Redundancy

(IT) Redundantly wired Ethernet networks are not uncommon. Protocols used for maintenance of these networks are STP (old and slow), RSTP (not so old and not so slow), and many vendor-specific protocols.

(OT) Redundant networks are common, but they are often wired in a ring instead of a mesh. This allows for rapid recovery times, down to milliseconds, in order not to get any disturbances in the operation of an OT system. The protocols used for operating the ring are very vendor-specific, and there are dozens of them. RSTP can be found in non-demanding applications.

3 PC's

Usage

(IT) PC's everywhere, using either Microsoft Windows or Apple macOS.

(OT) PC's are used in the higher levels of an industrial automation system, i.e. operator consoles, engineering software, distributed control systems (DCS), but not at the lower levels. Usually this runs on Windows.

Type of PC

(IT) No special requirements.

(OT) Industrial PC variants, with sturdy housing, rack mounted, temperature range, shock proof, no ventilators, etc. to allow usage in physically demanding environments.

4 Software

Windows versions (desktop)

(IT) The latest version of Windows is used, or the version before that.

(OT) It is quite common to find rather old Windows versions, such as XP and sometimes even NT. This is caused by the long time industrial equipment remains in use, and additionally by the relative slowness of industrial vendors to keep up with Microsoft.

Windows versions (embedded)

(IT) There is no need to run anything other than the full Windows.

(OT) A trimmed-down version of Windows called "Windows Embedded" or "Windows CE" is often installed on embedded systems. It only contains those parts of Windows that are needed for the application software on it, so it can be run on cheaper hardware (less memory, slower CPU, smaller disk).

The license costs are also considerably lower, making it attractive for product vendors of embedded and IoT devices.

The Telegraph

HMS Queen Elizabeth is 'running outdated Windows XP', raising cyber attack fears

Follow

By Danny Boyle and Ben Farmer, DEFENCE CORRESPONDENT

27 JUNE 2017 • 10:26AM

Fears have been raised that Britain's largest ever warship could be vulnerable to cyber attacks after it emerged it appears to be running the outdated Microsoft Windows XP.

As HMS Queen Elizabeth left its dockyard for the first time to begin sea trials, it was revealed the £3.5billion aircraft carrier is apparently using the same software that left the NHS exposed.

Screens inside a control room on the ship, which is the largest vessel ever built for the Royal Navy, reportedly displayed Microsoft Windows XP - copyright 1985 to 2001.

Linux

(IT) Linux is extensively used, not necessarily on desktop PC, but more on servers and other infrastructure equipment.

(OT) Linux is seldom used as a platform for industrial control software itself. However, it is extensively used in embedded applications, such as PLC's, without the users knowing Linux is inside.

Programming languages

(IT) C/C++, Java, JavaScript, Python, SQL, Go, and many others.

(OT) IEC-61131 languages (Ladder, SFC, Instruction List, Sequential Function Charts, Structured Text), C/C++, Python.

SCADA

(IT) Does not use SCADA.

(OT) Makes extensive use of SCADA packages, to show the operational state of an OT system. Operators can use it to control the OT system.

Note: in hackers terminology, "SCADA" means: an OT system. But in the OT world, SCADA is only a small part of an OT system.

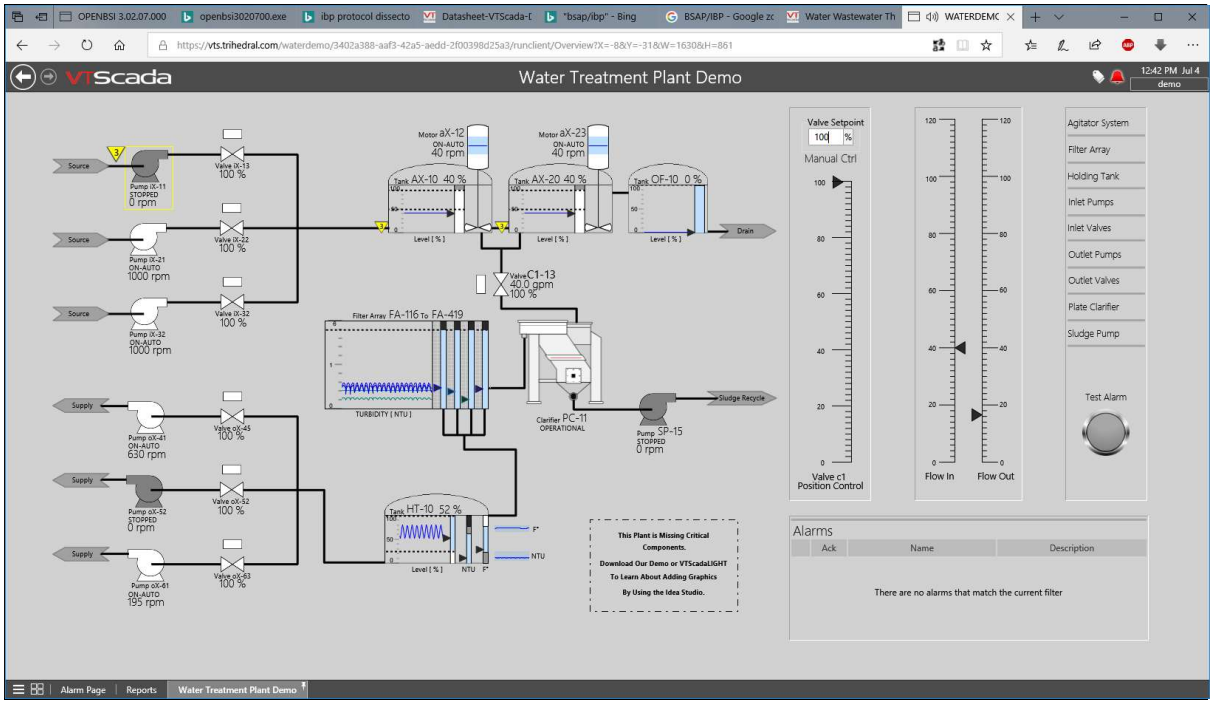


Figure: example of a SCADA screen, schematically showing the installation

5 Cybersecurity

Awareness

(IT) The awareness about cybersecurity is higher than in OT-environments.

(OT) The awareness about cybersecurity is generally lower than in IT-environments.

Firewalls

(IT) Commonly used.

(OT) Found at the higher levels of an industrial automation system, where blocking malicious traffic does not cause problems with the system. Also, many firewalls do not support the industrial protocols found in OT (with a few exceptions), and/or cannot handle the real-time requirements asked by OT protocols.

Internet connectivity

(IT) Always.

(OT) In principle it is not needed, an OT-system should be designed to have no need for internet connectivity. But in practice fully "air gapped" systems do hardly exist.

Password complexity

IT: Passwords are subject to a lot of rules in many organizations: length, usage of upper/lowercase and special characters, regular change, no re-use of old passwords, etc. Also, when the wrong password is used too often, an account can be blocked (locked-out).

OT: Passwords are a nuisance. Password complexity rules can often not be set. Machines and equipment often have the same password, often the factory settings, for years on end. It is unpractical to change the password, since the same equipment is controlled by multiple persons, each using the same 'user'name and thus also the same password. When multiple devices or machines of the same vendor are present, it is likely that they all have the same username/password combination. These are also not changed when a user/operator leaves the company.

Change of passwords

(IT) Users need to regularly change their password, as per company policy.

(OT) Passwords are seldom, if ever, changed. They are also often shared between people, i.e. everyone working as operator knows the same account and thus knows the password.

Multifactor authentication

(IT) Becoming the standard, if not already.

(OT) Many OT devices have no support for MFA.

Account lockout

(IT) When a user enters the wrong password several times in a row, the login account is "locked out". The user cannot use the account anymore until a system-administrator has released the account again, *or* a certain time-period has expired.

(OT) A login account of certain critical functions is *never* locked out. This would be very dangerous, as an operator then loses the capability to control his equipment. Also, with 24/7 shifts in a production environment, an IT administrator is not always available to help unlock an account.

Virus scanner

(IT) Virus scanners or an endpoint detection ?? are standard on Windows PC's,

(OT) Virus scanners on an industrial controller are scarce. Many owners assume that a virus scanner will slow down the system, or introduce errors because the processor cannot respond in time to certain events because the virus scanner is using the processor. Even though modern virus scanners do not heavily use the processor, this is still not believed.

But even so, running a virus scanner on an industrial controller does not always make sense. The usage of 'old' Windows versions is a problem, because the antivirus-companies may not support their products anymore. The virus signatures are no longer updated, and the system is no longer protected against modern malware.

And even if it could recognize modern malware, the virus scanner must regularly retrieve new signatures from a server on internet. But for this an active internet connection must be available, which is a danger in itself in OT environments.

WiFi

(IT) Most companies have WiFi in use, if not for own staff then for use by guests. The higher the speed of WiFi the better, so modern versions of WiFi are deployed (802.11n and up). Coverage is everywhere in the building.

The WiFi access points usually allow access via laptops and tables to all internal PC's, printers, servers, etc. Bluetooth is not used for this, because of its low bandwidth. Bluetooth is available too, either wireless headsets, wireless keyboards or mice, or for personal devices of staff (mobile phone, smart watch, etc.).

(OT) If WiFi is available, this is usually to support staff allowing access to the company LAN. WiFi can be used for control purposes, but only for non-realtime applications or very slow systems. This is necessitated by the unpredictability of WiFi with regard to delivery of network messages.

USB Usage

(IT) In general this is not seen as an issue, although there is a trend to disallow it.

(OT) USB is not commonly available on many OT devices, but when it is, there is a trend to disallow it.

USB has become the standard mechanism to transfer data between PC's and OT-equipment, where we saw floppies two decades ago.

6 Patching and updating

Software support period

(IT) Because of the short lifecycle of IT-equipment, the vendors make patches available for a few years, and then stop the support of their product.

(OT) The lifetime of OT products is often much longer than their support period. So, many vendors do not to support their product with patches for recently discovered vulnerabilities. No information can be found on the website, and there is no procedure for reporting vulnerabilities.

Installing of patches

(IT) Patches are installed as quickly as possible, in many cases automatically. When a reboot is necessary this can be done after working hours, or in the weekend

(OT) Patches are installed slowly, or not at all. This is caused by the fact that often devices need to be rebooted, which is not possible on 24/7 production systems. Only during a production stop (scheduled) is a patch installation + reboot possible. This may mean that there can be a long period between patch release and patch installation.

In some types of applications, patches may be installed but then the application software must be re-certified.

Automated installing

(IT) Many software packages now automatically scan the servers of their vendors for the availability of new patches, and if so, start downloaded these in the background and then automatically install them at the first opportunity. In case a reboot is needed this can be done at a appropriate moment.

(OT) Patches cannot be installed automatically, as this would cause a reboot at a completely unexpected moment. Also, automated installers need internet access, which is not always available in an OT environment (or when it is: it is most unwanted).

Automated installing is also not possible for smaller (usually embedded) devices, as the user must manually set the device in a mode suitable for installing a patch, i.e. toggle a switch, connect a laptop, insert a USB-stick, and power-cycle the device.

Patch frequency

(IT) Many vendors now follow a monthly or bi-monthly cycle, in which all new patches are published simultaneously. This is done to aid the system administrators, who can anticipate their arrival, this in contrast to the old situation, where patches arrived at apparently random moment many times per month.

(OT) Large automation vendors also follow a monthly or bi-monthly cycle, because there are enough vulnerabilities. Smaller vendors often have many months without any new patches, and so if there is one, release it immediately.

Testing patches

(IT) Often not done because of the automatic installation.

Figure: Not testing patches may miss bugs and affect users (source: X)

(OT) Some vendors do not allow their customers to patch any software without prior approval of the vendor. They test a patch first, to be sure it has no negative influence on their software. Only after their approval may customers install it.

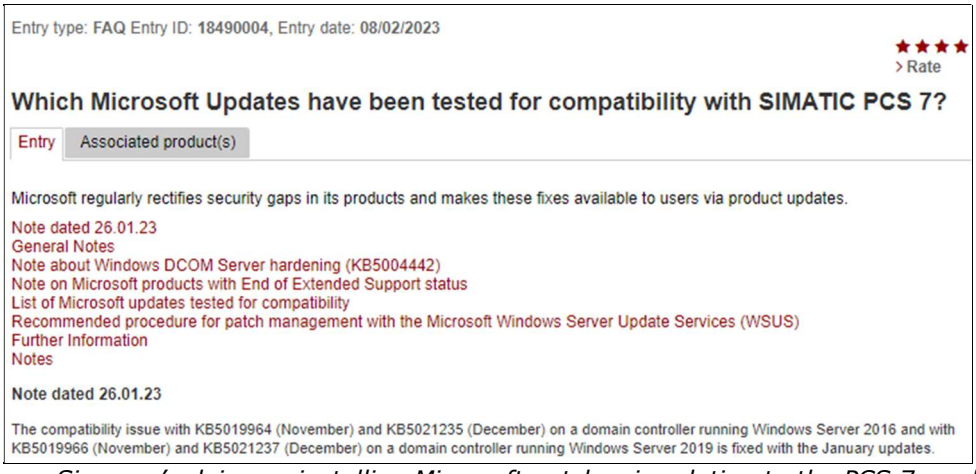


Figure: Siemens' advice on installing Microsoft patches in relation to the PCS 7 product

Reboot of equipment

(IT) Rebooting device is usually not problematic – this can be done in the evening or in the weekend, when nobody is working.

(OT) Rebooting devices is problematic, especially in 24/7 production environments. When a device needs to reboot, a production system cannot function, and thus the reboot can only be done on scheduled moments, for example during planned maintenance once every two years between Christmas and New Year's Eve.

Summary

This article is likely not complete in describing all possible IT/OT differences
If you have any suggestions, comments or additions,
please do not hesitate to contact me (email: rh[at]enodenetworks.com).