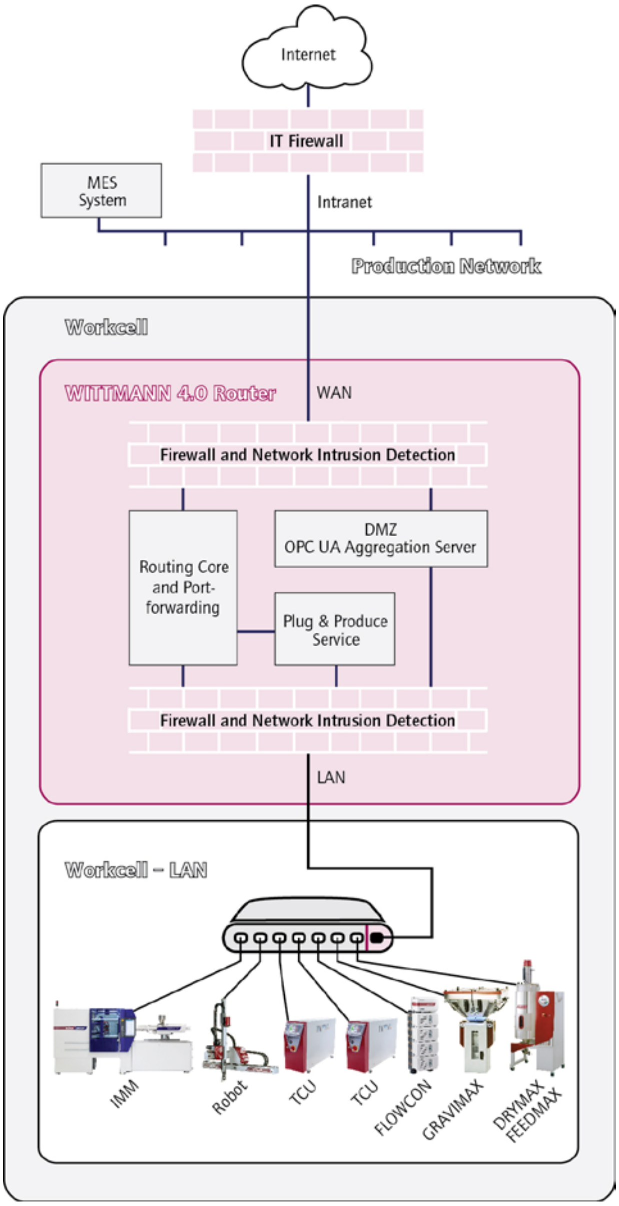
www.wittmann-group.com

NEWS RELEASE: TECHNICAL CONTRIBUTION September 7th, 2017

[Witt-NR-12-2017_cyber-security]

WITTMANN Group injection molding machines, robots and peripheral equipment for maximum cyber security

In the Industry 4.0 era – or more generally speaking, in the midst of the "digital transformation" currently taking place in the world – the networking of injection molding machines, robots and peripheral equipment is proceeding apace. We now have to meet the challenges faced in the field of plant security.



Reports of attacks involving the WannaCry ransomware and similar malware really woke up plastics processors to the issue of security when it comes to cyber-physical systems and facilities. After all, the WannaCry case resulted in numerous very well-known companies suffering the worst case scenario for a manufacturing operation, namely an unplanned production shutdown for an unforeseeable period of time. Like other malware before it, WannaCry worked by exploiting a security vulnerability in the Windows™ operating system.

The WITTMANN 4.0 security concept

It is common knowledge that the most fundamental aspect of any security concept is regularly performing software updates so that above all the operating system is kept up to date. While doing this does not afford complete protection, it is nevertheless an important basic step. Performing updates automatically is not, however, feasible for production systems, since an update can have unforeseeable consequences for the functionality of the connected machinery or device. In the worst case scenario, an automatic update may end up causing a machine to shut down, leading to the dreaded loss of production. As such, production systems in an *Industry 4.0* environment remain especially at risk and susceptible to any vulnerabilities in the operating systems in use being exploited.

WITTMANN BATTENFELD injection molding machines with B6 and B8 controls as well as robots with the latest R9 control from WITTMANN prevent the operating system from being permanently compromised by viruses due to the fact that changes that affect the system are saved to an internal RAM disk via a Unified Write Filter mechanism. This makes it possible to restore the device’s operating system to its factory defaults each time the system is booted up. Because of this, viruses cannot become “embedded” in the system and affect it permanently.

WITTMANN BATTENFELD has nevertheless tackled the wider issue of security and, in close cooperation with one of the leading cyber security companies in the industry, developed a security concept for networked WITTMANN 4.0 workcells that has already been implemented in the field. The development work was based on the assumption that the production network outside a WITTMANN 4.0 workcell could be compromised in terms of security even though the operator is naturally sitting behind a firewall. This is why the system architecture of a WITTMANN 4.0 workcell is designed according to the onion principle.

The firewall of the customer’s network forms the outermost layer surrounding the WITTMANN 4.0 workcell. Because the security mechanisms and settings there are unknown to the manufacturing cells, this layer must be regarded as being “unsafe”. The next security layer is formed by a restrictively configured WITTMANN 4.0 firewall that is installed in a router specially developed for the purpose by WITTMANN. The software on the router is digitally signed and every step of the router’s boot routine is designed to be “secure”. This precludes an attack being made via a software update. In contrast to conventional off-the-shelf firewalls, the WITTMANN 4.0 firewall is tailored to the specific purpose of each device and function that may be expected to be a component of the workcell. The configuration of the firewall is therefore especially restrictive. With the exception of the OPC protocol, which is used for communication with an MES or ERP system via OPC UA, all communication ports are closed by default and can only be opened from within the workcell, and only by the operator performing specific, intentional steps.

Communication with “the outside world”

WITTMANN BATTENFELD injection molding machines with B8 controllers, for example, can create an external connection via TeamViewer in order to make remote servicing functionality available, if desired. Having established a session, remote servicing allows a WITTMANN BATTENFELD office direct access to the authorized injection molding machine for the purpose of analysis.
Manual authorization can likewise be issued for the WITTMANN Group’s *QuickLook* App. This allows an Android or iOS mobile device within the company’s network to view the machine status of WITTMANN BATTENFELD injection molding machines with B6 and B8 controls and WITTMANN robots with R8.3 or R9 controls. In this case, the WITTMANN 4.0 router tells the *QuickLook* App on which ports which machines and robots can be found.
Every opening of an additional communication port does, of course, create another loophole and thus increases the potential risk of cyber attacks. Opening a port is, however, a deliberate act performed by the operator and the port only stays open for the duration of intended use.

Protection against DoS attacks

Another advantage of the WITTMANN 4.0 system architecture is that it protects production systems against so-called DoS (Denial of Service) attacks. These typically attempt to bombard the remote station with such an immense flood of requests that it may no longer be able to cope with its communications tasks and shuts down.
If this flood of communications packets reached a production machine directly, it could well result in the machine shutting down completely. Within the WITTMANN 4.0 architecture, however, the only thing that may possibly shut down would be the router and thus only the communications with the MES/ERP system, though it may be assumed that this system would no longer be active at the time either due to network overload. The processing machines and other equipment within the affected WITTMANN 4.0 workcell are able to continue working unhindered, however.
Over and above this, there is a basic protective mechanism in place intended to prevent the WITTMANN 4.0 router from shutting down in the case of a DoS attack. A special feature of the WITTMANN 4.0 router is that it is able to “estimate” the volume of communication traffic the internally networked devices typically have with an external MES/ERP system. The communication frequency of production equipment is known within certain bounds and can be predicted by dint of the OPC UA protocol used here and the coming EUROMAP standards based on it. Should this frequency vary atypically over the medium term, it must be assumed that there is an anomaly, such as a DoS attack. As a counter measure, the WITTMANN 4.0 router closes the socket being used for communication in order to prevent the socket being attacked. The functionality of the router is thereby maintained.

WITTMANN 4.0: “Plug & Produce”

At the core of a WITTMANN 4.0 workcell is a WITTMANN BATTENFELD machine with B8 controller, WITTMANN robot with R8.3 or R9 controller and the various WITTMANN peripheral devices. This zone is shielded from the outside world, thus allowing for secure operation with the operating system version supplied with the equipment.

The latest peripheral devices from WITTMANN can be plugged in and out of a WITTMANN 4.0 workcell according to the “Plug & Produce” principle at will. After a newly attached peripheral device has been server authenticated by means of SSL/TLS protocol and key exchange via certificate, device identification is performed. The newly attached device identifies itself and is registered in the device list of the WITTMANN 4.0 router with the corresponding identifiers. The device list acts as a database that is used by the B8 controller of the WITTMANN BATTENFELD injection molding machine to configure the newly attached device.

The peripheral devices have their own passwords that are used for logging in. Each device is supplied with a default password that can, and indeed should, be changed by the operator. The responsibility for password security lies with the respective operator, particularly as there are no factory default master passwords. The login process takes place using the previously established secure SSL connection.

The actual data exchange between the various attached devices and ultimately to an MES or ERP system takes place via the standard OPC UA protocol. Communication between the injection molding machine and the MES system will in future be updated to use the EUROMAP 77 standard as soon as it is released – probably in September 2017. Various EUROMAP standards for the peripheral device communication via OPC UA are already in the standardization phase and will be implemented immediately they become available.

Every WITTMANN 4.0 workcell is equipped with the aforementioned components and security mechanisms as standard so as to provide the operator with the best possible cyber protection and maximum machine and device availability.

Over the course of numerous tests conducted by the cyber security company commissioned by WITTMANN, simulated attacks using a variety of different threat scenarios were acted out and tested by “white-hat” hackers. WITTMANN 4.0 proved itself to be robust in all scenarios and enabled production to continue uninterrupted within the entire workcell.

(Johannes Rella,
Head of the Software Development Department at WITTMANN Kunststoffgeräte GmbH in Vienna)

The WITTMANN Group is a worldwide leader in the manufacturing of injection molding machines, robots and peripheral equipment for the plastics industry. Headquartered in Vienna/Austria, the WITTMANN Group consists of two main divisions, WITTMANN BATTENFELD and WITTMANN, which operate 8 production facilities in 5 countries, including 33 direct subsidiary offices located in all major plastics markets around the world.

WITTMANN BATTENFELD focuses on the independent market growth in the manufacturing of state-of-the-art injection molding machines and process technology,

providing a modern and comprehensive range of machinery in a modular design that meets the actual and future requirements of the plastic injection molding market. WITTMANN's product range includes robots and automation systems, material handling systems, dryers, gravimetric and volumetric blenders, granulators, mold temperature controllers and chillers. With this comprehensive range of peripheral equipment, WITTMANN can provide plastics processors with solutions that cover all production requirements, ranging from autonomous work cells to integrated plant-wide systems.
The syndication of the WITTMANN Group has led to connectivity between all product lines, providing the advantage plastics processors have been looking for in terms of a seamless integration of injection molding machines, automation and auxiliary equipment – all occurring at a progressive rate.

Contact:

WITTMANN Kunststoffgeräte Ges.m.b.H
Lichtblaustrasse 10
1220 Vienna
AUSTRIA
Tel.: +43 1 250 39-0
info.at@wittmann-group.com
www.wittmann-group.com

WITTMANN Robot Systeme GmbH
Am Tower 2
90475 Nuremberg
GERMANY
Tel.: +49 9128 7099-0
info.de@wittmann-group.com
www.wittmann-group.com