Cyber safety – what happens next

Ratingen, Germany, 26th February 2013

The high profile incidents with the Stuxnet malware and vulnerable SCADA systems provided a timely reminder that we need to take effective measures to protect process control systems and infrastructure from attacks from cyberspace. Thomas Lantermann, Senior Business Development Manager at Mitsubishi Electric Europe B.V., Factory Automation – European Business Group, looks at where vulnerabilities lie and how the problem will be exacerbated in the future, and looks at new security standards that offer protection.

Cyber criminality is developing into a danger which should be taken ever more seriously, and which is assuming sometimes unimagined dimensions. High profile incidents involving malware have shown that the typical automation architecture has weak points and vulnerabilities when it comes to security, and this is leading many companies to question the traditional methods used to move information around, in particular from the plant/asset level to the enterprise level.

Today, Mitsubishi Electric is already working on developing new security standards. Consideration is also being given to very basic gaps in security such as unprotected connections to the Internet. Corresponding protective measures which support systematic IT security and minimise the area open to attack for viruses, worms and Trojans are indispensable.

When we look at the attacks from the Stuxnet malware, what we see is that it changed the point of attack on a business from the seemingly secure top end to the somewhat vulnerable middle ground – the PC hardware and software that lies between the plant floor control systems and the higher level enterprise

systems. In particular, there are the communications gateway systems that exist to provide an information bridge between the plant floor and the wider enterprise systems. Mitsubishi Electric has identified these gateway systems as a major point of weakness in system security, vulnerable to attacks from outside, as well as to viruses brought in accidentally on CDs, memory cards and USB sticks.

Being networked, and containing software to influence the control layers below and the information layers above, these PCs are often attractive targets to anyone the outside world looking to disrupt operations. Coupled to this is the fact that many of these PCs may well have been poorly maintained in terms of security patches, or will be running unsupported legacy versions of operating systems, raising the risk factors considerably.

Many IT security systems are designed to mitigate against attacks on PC-based systems. However, these solutions are more focused on dealing with the problem and protecting the weak points than understanding how the problem might have occurred and eliminating the weak points.

Mitsubishi Electric’s approach is somewhat different, with the objective of separating these mass storage devices such as PCs from the operating system, and only retaining peripheral drivers which are relevant to control. To do this, technology is needed which challenges the traditional automation architecture.

Rather than having a layer of gateway PCs in the automation structure, instead, the required software tools are integrated on an already existing robust hardware platform such as the PAC platform. Mitsubishi Electric addresses the requirements for control and information that would previously have existed as PC software in the gateway layer through products and solutions such as MES-IT, C Connector, C Batch and remote terminal units (RTUs).

The IT interface module MES-IT, which Mitsubishi Electric has developed jointly with e-F@ctory Alliance Partner ILS Technology, represents an uncomplicated, direct connection from process systems at field level to ERP or MES databases and systems at company level. It collects production data and test results in each phase of production and transfers the data directly to higher level systems. This means that quality control can be improved. Decisions based on real time information can also increase profitability. Traceability is also extremely high here: each product manufactured, regardless of whether it is still in the production process or is already in the warehouse, can be followed up accurately and the material flow can therefore be controlled more precisely.

Similarly to MES-IT, the PAC module C connector supplies real time information from the whole automation system directly into the user's SAP system. However, this solution can be operated even more intuitively due to preconfigured templates. The module simplifies cross-platform, vertical integration of the production level in MES and ERP systems through a bi-directional data exchange. Here, too, the PC, as a gap in security, is consciously dispensed with. Efficiency is increased, as products can be manufactured practically 'on demand'. Time and costs can be saved because of the ease with which the system can be installed and integrated. An IT specialist is not needed. Even additional components such as controllers or RFID readers from other manufacturers can be integrated quite readily.

A solution for the control of batch processes in real time is the batch control system, C Batch, from Mitsubishi Electric and INEA, another e-F@ctory Alliance partner. As an easy to integrate, rapid and cost-effective batch management solution, it reduces the complexity of traditional process control architectures considerably. The batch system is not PC based either, but is based on a standard control platform. The flexible system can execute several recipes in parallel, and the recipe parameters are precisely scaleable to requirements.

This means that rejects and waste can be kept to a minimum. Lines and plants are configured and not programmed, recipes can easily be reused and compliance with ISA standards such as S88 becomes easier as C Batch was designed to comply from its inception.

All of these innovative technologies create the possibility of removing the gateway PC from the enterprise topology altogether. By eliminating the PC level, additional crash security and a high transfer speed are guaranteed as well as mitigating from the dangers from cyberspace.

The fact that users are frequently completely unaware of gaps in security was made clear in 2006 by German company NESEC Gesellschaft für angewandte Netzwerksicherheit in a study entitled “Hacking SCADA/SAS Systems“. This study showed that many companies wrongly assume that their SCADA systems are not connected to the Internet and are therefore safe. In fact, the systems tested in the study were certainly connected to the Internet and were wide open to malware. (http://stuweb.ee.mtu.edu/~ssmoily/NESEC.pdf)

Photo Caption: Mitsubishi Electric offer innovative technologies that create the possibility of removing the gateway PC from the enterprise topology altogether. By eliminating the PC level, additional crash security and a high transfer speed are guaranteed as well as mitigating from the dangers from

cyberspace.

About Mitsubishi Electric:

With 90 years of experience in providing reliable, high-quality products to both corporate clients and general consumers all over the world, Mitsubishi Electric Corporation is a recognized world leader in the manufacture, marketing and sales of electrical and electronic equipment used in information processing and communications, space development and satellite communications, consumer electronics, industrial technology, as well as in products for the energy sector, water and waste water, transportation and building equipment.
With around 117.000 employees the company recorded consolidated group sales of 36,3 billion Euro* in the fiscal year ended March 31, 2012.
Our sales offices, research & development centres and manufacturing plants are located in over 30 countries.
Mitsubishi Electric Europe B.V., Factory Automation European Business Group (FA-EBG) has its European headquarters in Ratingen near Dusseldorf, Germany. It is a part of Mitsubishi Electric Europe B.V., a wholly owned subsidiary of Mitsubishi Electric Corporation, Japan.
The role of FA-EBG is to manage sales, service and support across its network of local branches and distributors throughout the EMEA region.

**Exchange rate 109,56 Yen = 1 Euro, Stand 31.3.2012 (Source: Deutsche Bundesbank)*

Further Information:

www.mitsubishi-automation.com

www.mitsubishielectric.com

Mitsubishi Electric Europe B.V.
Factory Automation European Business Group
Monika Torkel
Marketing Communications Coordinator
Gothaer Str. 8
40880 Ratingen, Germany
Tel.: +49 (0)2102 486-2150
Fax: +49 (0)2102 486-7170
Monika.Torkel@meg.mee.com

PR agency:

DMA Europa Ltd.
Mr. Roland Renshaw
2nd Floor, Snuff Mill Warehouse
Park Lane, Bewdley.
Worcestershire. DY12 2EL, UK
Tel.: +44 (0)1299 405454
Fax: +44 (0)1299 403092
roland@dmaeuropa.com www.dmaeuropa.com