Cyber-security in the emerging digital world

Comment from: Chris Evans, Marketing & Operations Group Manager, Mitsubishi Electric Europe B.V. Automation Systems Division

It seems a long time ago now since various malware attacks on the operational layer changed the security landscape and highlighted vulnerabilities in the de-facto automation architecture. However, as we move along the road towards Smart Manufacturing with a view to improving efficiency, productivity and reliability of supply using the principles of Industry 4.0 and the Industrial Internet of Things (IIoT), the subject of cyber-security is becoming arguably even more important.

Smart Manufacturing relies on a greater convergence of the IT and OT layers of a business and if that is applied to an existing plant, it would be reasonable to assume that the potential for cyber-attack, if not understood and mitigated against would be higher.

If we were designing a new plant on a greenfield site, it would be relatively easy to build it while being mindful of all the current cyber-security issues and vulnerabilities. The reality is that most manufacturing plants in the UK have been around a long time and most of the automation considerations are centred around productivity not cyber-security. In this existing industrial landscape, it was realised that control systems were potentially vulnerable, often due to out of date or poorly maintained operating systems and CD drives or USB ports that had not been locked down.

Cyber-security is an arms race of escalating capabilities, so 'defenders' of vulnerable assets must see it as a journey rather than a destination, constantly reassessing the situation and implementing new defences whenever necessary. This is against the background of developing technologies and requirements that mean control systems are always becoming bigger, more complex, more distributed and increasingly open.

To be successful the defence strategy against cyber-attack must be seen in a holistic way and needs to happen at all levels of the enterprise. This must start at the plant level and automation equipment manufacturers must look to build in security as a natural part of the design process.

For instance, PLCs (programmable logic controllers) need to include multiple embedded features such as hardware security keys and multi-layer password structures.

Use of hardware security key authentication prevents programs from being opened or edited on unapproved personal computers that have not been "bound" to the security key. PLC CPUs can also be paired to the security key and programs will not run unless this hardware match exists. This also has the benefit of protecting the intellectual property of the control system. Additionally, IP filtering should be used to register the IP addresses of devices approved to access each PLC or HMI (Human Machine Interface). This makes unauthorised access much more difficult.

Whilst end users will want maximum security; they will also continue to insist on simplicity of operation. Some of these automation security measures, all of which are optional, could be argued to complicate operations and that is why a holistic view of security needs to be taken, considering all aspects of the operation. It may be that in some areas, some measures can be relaxed for the sake of continued operations and this is fine provided that the risk has been assessed and counter measures are implemented elsewhere to alleviate the threat. As with everything related to cyber-security the consideration has to be probability and risk, security and operational systems should be designed around these important criteria.

It is probably an unchangeable aspect of the human condition that some people will always seek unauthorised access to control systems. Therefore, manufacturers and control engineers must build security measures into their products and systems and recognise that these are surmountable hurdles rather than impregnable barriers, so must be constantly renewed and redeveloped.

Image 1: As we move along the road towards Smart Manufacturing the subject of cyber-security is becoming arguably even more important.

[Source: Mitsubishi Electric Europe B.V.]

Image 2: Chris Evans, Marketing & Operations Group Manager at Mitsubishi Electric.

[Source: Mitsubishi Electric Europe B.V.]

Note to Editor: if you would like the text in another language please contact Carolin Heel at DMA Europa – carolin@dmaeuropa.com.

About Mitsubishi Electric

Corporation (TOKYO: 6503) 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, energy, transportation and building equipment. Embracing the spirit of its corporate statement, Changes for the Better, and its environmental statement, Eco Changes, Mitsubishi Electric endeavors to be a global, leading green company, enriching society with technology. The company recorded consolidated group sales of 4,444.4 billion yen (in accordance with IFRS; US$ 41.9 billion*) in the fiscal year ended March 31, 2018.

Mitsubishi Electric Europe, Industrial Automation – UK Branch is located in Hatfield, United Kingdom. It is a part of the European Factory Automation Business Group based in Ratingen, Germany which in turn is part of Mitsubishi Electric Europe B.V., a wholly owned subsidiary of Mitsubishi Electric Corporation, Japan.

The role of Industrial Automation – UK Branch is to manage sales, service and support across its network of local branches and distributors throughout the United Kingdom.

**At an exchange rate of 106 yen to the US dollar, the rate given by the Tokyo Foreign Exchange Market on March 31, 2018*

Further Information:
Website: gb3a.mitsubishielectric.com

Email: automation@meuk.mee.com

Facebook: www.facebook.com/MEUKAutomation

Twitter: twitter.com/MEUKAutomation

YouTube: www.youtube.com/user/MitsubishiFAEU

LinkedIn: www.linkedin.com Mitsubishi Electric - Automation Systems UK

Editor Contact

DMA Europa Ltd. : Carolin Heel

Tel: +44 (0)1562 751436
Web: www.dmaeuropa.com
Email: carolin@dmaeuropa.com

Company Contact

Mitsubishi Electric Europe B.V. Automation Systems Division : Garry Lewis, Manager - Marketing & Communications

Tel: +44 (0) 1707 288769
Fax: +44 (0) 1707 278695
Web: gb3a.mitsubishielectric.com
Email: automation@meuk.mee.com