The importance of security in an increasingly connected world

By Mark Fairhurst.

Digital communication and the opportunity for more interconnectivity that it brings is a catalyst for greater access to, and the democratisation of, information. Although this is a force for good, having easy access to information can also have volatile and unpredictable negative consequences.

In this article the author offers a personal view on the positive impact this is already having on the fluid power industry and raises questions on how we balance the need for regulation with freedom of choice when considering industrial applications.

Moving beyond power transmission

Traditionally, fluid power systems have concentrated on power transmission. Hydraulic systems were mainly made up of control valves, power unit, hydraulic actuators and fluid monitoring equipment. Pneumatics systems typically comprised a power unit, fluid conditioning, actuators and control valves.

Today, fluid power systems are not only about power transmission, but also motion control, with a focus on motion that is more precise and predictable.

At a local level this can involve electro-hydraulic or electro-pneumatic actuation, which is in turn, part of a network of many individual components that are able to communicate with each other within a wider system.

The communications process need not only be autonomous and operating within the particular system in question; indeed the system, or components within the system, can also communicate with a much wider network.

Through the use of sensors and wireless technology, this digital interconnectivity means that plant control and monitoring need not be confined within the walls of a physical building and could feasibly be undertaken from anywhere in the world.

▲ **Mark Fairhurst: "The world is becoming an increasingly unpredictable environment, and so the issue of security risk should not be taken lightly."**

As a result, a plant controller or maintenance engineer no longer has to be in regular close proximity to the plant and equipment in order to control and monitor its operation.

The implications of a wider network

So, with all this increased motion control and communications know-how many modern fluid power systems have grown to become part of a much wider network. This wider network scenario is, in essence, very much part of the Industry 4.0 revolution where disruptive technologies can bring new functionalities into the marketplace.

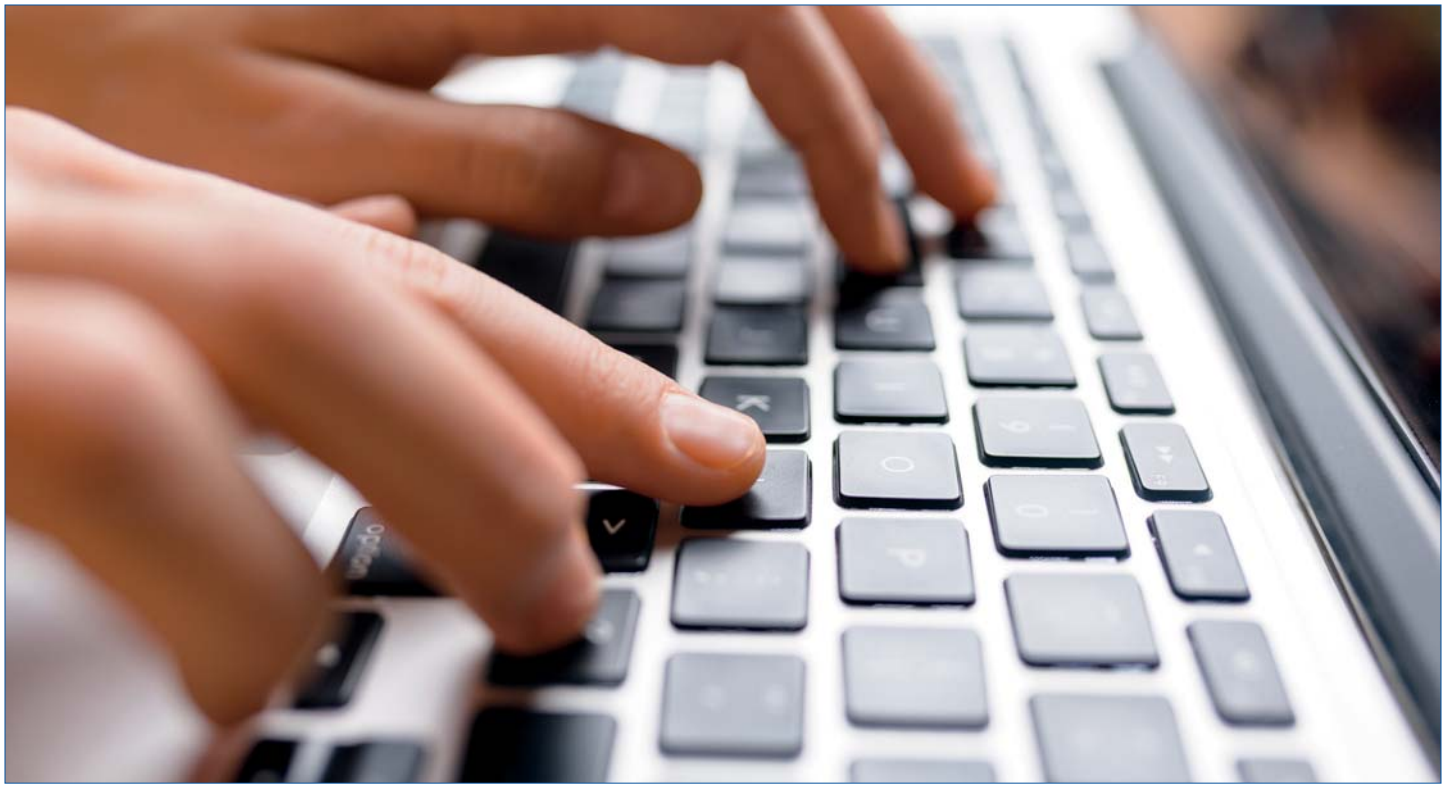
The overriding benefits of having easy access of information, often in real-time or near real-time, are many. For example, sensors within a system can automatically inform a maintenance engineer when a component or larger piece of equipment has malfunctioned or is due for replacement by sending an alert to his or her smartphone, tablet or PC. The maintenance engineer can also remotely interrogate particular equipment within the system in order to, for example, change its function, hours of operation, schedule maintenance procedures, or investigate its operational history and which personnel operated certain types of equipment during specific periods.

However, these changes can expose weaknesses in regulations and controls. In the digital world, they are often highlighted through security breaches. In 2016, 46% of UK SMEs suffered a cyber security breach.

Managing security effectively

Nonetheless, with all these benefits and more to be had from today's integrated high-tech motion control systems – whether from an operational or maintenance and overhaul perspective – certain important choices and decisions need to be made. Some of the most important of these revolve around security. Understandably, there needs to be clear procedures about who should be allowed to access the system, or parts of the system. Making decisions in terms of operating, maintaining or making changes to the system and the wider network also requires clarity and structure.

Moreover, making this type of decision regarding individual access to, and mandate to control the system is just the start. Only certain people may have been given the authority to do certain things, or have access to certain types of information. This therefore requires careful control and monitoring of communication protocols around information kept within the system,



▲ **Careful thought needs to be given about who should be allowed to access the system, or parts of the system, and be able to make decisions in terms of operating or maintaining or making changes to the system and the wider network.**

otherwise it could be open to infiltration or malicious abuse by other parties.

Safety first

In this regard the biggest concern is that if people are able to maliciously intercept these communication systems it may not be long before a serious injury or even a fatality results. It could be due to motion equipment in a bottling plant becoming unstable; it could be the result of robotic arms flailing in precarious ways; it could be due to a shock from a power transmission system, and so on.

In the wake of a serious injury or death, the subsequent court case could then set a precedent whereby a whole new level of cyber policing is put in place. If this were to become a reality, it could potentially stop the growth in further development and deployment of Industry 4.0-related systems technology in its tracks.

What steps can companies take?

It is vital that organisations understand how robust their data communication systems are. Some systems are likely to be more resilient than others.

For example, in a manufacturing plant a radio-frequency (RF) wireless transmission system could prove to be more reliable and robust than say Wi-Fi. This is because Wi-Fi is more open to being intercepted or corrupted at any level.

Accordingly, we need to reflect on what the implications are of moving forward too rapidly without having suitable levels of security in place.

It is also worth ensuring that any computer software used as part of the system has a reputation for being secure, and that proven encryption technology is deployed to make it impossible for malicious hacking to take place.

Additionally, companies should make sure that immediate IT-related help and advice is at hand in the event of any attempted security breach occurring. Furthermore, from a system design perspective, it is important that systems are thoroughly beta- tested in the real world, in order to monitor their performance and resistance to security abuses.

Staying ahead of the curve

In a volatile world, cyber security is an issue for all. It is therefore all the more important that we should develop efficient, reliable and robust motion control systems in order for them to conform to the best ideals of Industry 4.0 without risk of compromise. Industry 4.0 is already here and the trend is likely to gather even greater momentum over the coming months and years.

Thankfully these security issues are being addressed by information network providers and the like who have realised that the consumer internet and existing wireless platforms are not fully suitable for industry.

In fact, such is the speed of change that I advise those interested to keep a watchful eye on new government guidelines and news from trade associations such as the British Fluid Power Association (BFPA). Let's not let poor levels of security risk compromise the major improvements in efficiency, flexibility and reliability that this type of technology can offer.

About the author

Mark Fairhurst is a Technical Director at BHR Group. He is presently the Vice-Chairman the product testing committee of the BFPA/BSI, and the Chairman of the Technical Advisory committee of the Water Jet Technology Conference.

About BHR Group

BHR Group is an independent technology organisation providing engineering consultancy, industrial research and product development services for the energy & power, process and water & waste water industries.

Specialists in understanding how fluids behave, how they interact with each other and how they react with their surroundings, it designs, develops, validates and optimises processes for the benefit of its clients.

Originally established as the British Hydromechanics Research Association (BHRA) in 1947, and privately owned since 1989 it is based in Cranfield, Bedfordshire.