CHANGES IN THE NETWORK SECURITY LANDSCAPE

Security requirements for industrial Ethernet networks are quickly migrating from Enterprise networks to process control and other industrial environments. The recent issues with the Stuxnet malware has given us all a wakeup call, and we need now to take a fresh look at how security is managed within industrial networks. John Browett of CLPA looks at the potential threats to industrial network security, and how to mitigate them.

In the march toward Ethernet as the industrial network of choice, considerations for network security have lagged behind somewhat. And yet there is the very real possibility of networks being compromised both from outside a given facility, and from within.

Of course, the risk of deliberate hacking from within a company is difficult to protect against and is as much a personnel security issue than a general network security issue. Sensible security considerations however need to extend to the possibility of personnel accidentally connecting the wrong device to the wrong part of a network, or to unauthorized users finding themselves able to adjust key process parameters without realizing what it is that they're doing. In addition, as companies come to see the benefits of remote access to plants, monitoring processes by standard web browsers for example, then they are opening themselves up to the possibility of abuse of the network by third parties.

In particular, last year's incident involving the widely publicized Stuxnet virus that attacked SCADA (supervisory control and data acquisition) systems has shown that a typical plant floor control architecture has weak points and vulnerabilities when it comes to security. This has led many companies to question the traditional methods used to move information around between the plant/asset and the enterprise level.

The Stuxnet virus changed the point of attack in the business from the seemingly very secure top end to the somewhat vulnerable middle ground. At this level we frequently see PC-based control systems with little or no security implemented, and some technologies still being utilized despite known vulnerabilities.

Security problems at this level and at plant floor device level are exacerbated by the fact that there is often limited collaboration between a company's IT department and the control engineering departments. In addition, within the control and engineering community, there is not always adequate recognition of the automation system security threats and liabilities. In particular, the business case for automation system security is not established, and there is limited understanding of the automation system risk factors.

The drive towards open network technologies generally, and towards Ethernet in particular, as a means of giving companies the freedom they want to choose best of breed control technologies has exacerbated the security threat. Users want standardization, flexibility and choice, and this has been delivered through standardized open protocols. The trade-off, though, which is only just coming to be realized, is that these open protocols are less robust and more susceptible to attack. By contrast, the old proprietary networks were highly robust by virtue of their non-standardisation, but they were far less flexible and they ultimately limited product choice.

Looking then at what the ideal industrial network would offer, we can build up a wish list that offers the robustness of the old combined with the flexibility of the new. This wish list might include common cabling, standard connectors, open standards, ease of configuration, flexibility, highest possible security, and reduced susceptibility to attack.

In looking at how we might be able to adapt industrial Ethernet to meet the requirements of this wish list, it is worth revisiting our definition of Ethernet, because nowhere in networking parlance has a single word been so misused as an umbrella term for so many disparate standards, technologies and applications. And the best place to start for that is with the OSI seven layer model itself.

Layer 1, the Physical Layer, defines all the electrical and physical specifications for devices. In particular, it defines the relationship between a device and the physical medium. Layer 2 is the Data Link Layer, providing the functional and procedural means to transfer data between network entities and to detect and possibly correct errors that may occur in the Physical Layer. It is here that Ethernet is defined as a network protocol under the IEEE 802.3 standard.

Over the years, Ethernet has become synonymous with the TCP/IP suite, but one does not necessarily imply the other. IP is defined under the Network Layer (Layer 3) of the OSI model. This Layer provides the functional and procedural means of transferring variable length data sequences from a source to a destination via one or more networks. The Transport Layer (Layer 4) provides transparent transfer of data between end users, and defines the likes of TCP and UDP.

The Session Layer (Layer 5) controls the connections between computers, whilst the Presentation Layer (Layer 6) transforms the data to provide a standard interface for the Application Layer (Layer 7) at the top of model. It is here that you find typical applications such as FTP, HTTP, RTP, SMTP, SNMP and others. In short, when it comes to operating as a communications architecture in industrial networks, Ethernet is capable of very little without the layers that sit above it.

Not all industrial Ethernet offerings implement the Ethernet stack in the same way. Within the Application Layer the different industrial Ethernet organizations implement their own kernels and protocols which define much of the functional benefits of their technologies. From a security point of view, though, what is really of interest are the more vulnerable lower layers.

Under the seven layer model, all it takes is for one layer to fall to an attack before the whole communications system is compromised – potentially without the other layers even being aware that there is a problem. Security is only as strong as the weakest link.

There are a number of discrete security products available, and these work well, but one of the biggest problems in the industrial arena lies in implementing tightly integrated security systems without incurring excessive costs and without imposing a level of complexity that makes the system difficult to maintain and support. Further, standard commercially available security solutions are rarely up to the rigours of life in challenging industrial environments.

In terms of network technology, much work has been done to make Layer 2 more secure, but in classic implementations of industrial Ethernet little has been done to address weaknesses in the Network Layer (Layer 3) and the Transport Layer (Layer 4). Like the office Ethernet implementation, the vast majority of industrial Ethernet technologies are still built around IP within Layer 3 and TCP/UCP within Layer 4.

Most industrial Ethernet network installations implement perimeter security (firewall services) at points where they connect to other networks to provide protection at these vulnerable layers. Firewalls filter on source and destination IP addresses and protocol port numbers (for example TCP and UDP ports) to further restrict the traffic permitted to enter an Ethernet network. Packet filtering may be implemented even among known network communities, and in some cases filtering deals with very specific device addresses and application ports to provide a layer of access security unique to an attached device and application. Despite this however, in classic industrial Ethernet implementations, Layer 3 and Layer 4 are still highly vulnerable to attack.

CC-Link IE, however, is different. CC-Link IE (Control and Communication Link Industrial Ethernet) was developed by CLPA as the first completely integrated gigabit Ethernet network for industrial automation, defining the new threshold for open standards for Industrial Ethernet. CC-Link IE combines the best of many existing technologies and applies them to an optical or copper based industrial network system with a redundant architecture that enables extremely high-speed and reliable data transfer between field devices and other controllers via Ethernet links. The signalling rate of 1Gbps will redefine the users' expectations and systems capabilities; it being more than enough to cater for the real-time communications requirement of today's manufacturing industries.

There are variants of CC-Link IE to address control requirements at all levels of the automation network. At controller level, there is CC-Link IE Control. At device level, there is CC-Link IE Field and CC-Link IE Motion. And of course there is tight integration with the CC-Link fieldbus.

Most importantly, CC-Link IE differs from conventional implementations by defining an open "Real-Time Protocol" within the stack layers. By taking this approach to implementing these layers within the Ethernet stack, CC-Link IE realizes the benefits of our network technology wish list.

It uses standard Ethernet connectors, it is easy to configure and it is highly robust. It is also an open standard, so users still have that freedom of choice in the selection of best-of-breed component technologies. But most importantly from a

security point of view, it inherently offers the highest possible security and is therefore less susceptible to attack. These are significant advantages over alternative industrial Ethernet implementations. The key distinguishing factor is an open, but controlled knowledge base for the network technology. Hence while bona-fide companies can implement the technology on an open basis, it will be harder for the "bad guys" to infiltrate.

Security requirements for industrial Ethernet networks are continuing to evolve, with sophisticated requirements increasingly migrating from Enterprise networks to process control and other industrial environments. Wherever there are network installations, companies need to look at the probability of attacks to the network, and the risk associated with any attack. In every case, as security becomes more important, companies must look at ways to mitigate the risk, reduce the risk or eliminate the risk as appropriate within each branch of the network topology. With its open standards approach combined with proprietary communications technology, the CC-Link IE implementation of industrial Ethernet represents an extremely attractive option in the drive to maximize and optimize network security.

About the CLPA

The CC-Link Partner Association (CLPA) is an international organisation with over 1,500 member companies worldwide. The partners' common objective is promotion and technical development of the family of CC-Link open network technologies. Over 1,100 certified products are now available from over 250 manufacturers. CC-Link is the leading industrial fieldbus in Asia and is becoming increasingly popular in Europe and the Americas. The European headquarters is in Germany, with offices throughout the continent.

Editor Contact

DMA Europa Ltd : Bob Dobson

Tel: +44 (0)1798 861677
Fax: +44 (0)1299 403092
Web: www.dmaeuropa.com
Email: bob@bobdobson.com

Company Contact

CLPA Europe : John Browett

Tel: +44-(0)776 833 8708
Fax: +49 (0)2102 532 9740
Web: www.the-non-stop-open-network.com
Email: John.browett@clpa-europe.com