Defence-in-depth now takes in fieldbus levels

Between the centuries, Chinese emperors hiding behind the Great Wall and IT managers hiding behind the firewall have learned that dependence on a single point of security leads to a painful lesson in defeat. New technology offers a layered approach to network defence from the field level upwards. Eric Byres and Ian Verhappen

ARTWORK: FRANK OGDEN

As the famous military strategist Clausewitz once said, 'If you entrench yourself behind strong fortifications, you compel the enemy to seek a solution elsewhere.' The enemy of modern Ethernet-based control systems – the wily hacker or virus writer – will find a way around the firewall and into the critical computers and devices on the network if given any sort of chance.

The IT world has learned this lesson in very expensive ways. After years of infected servers and desktops costing millions of dollars in lost production, most IT departments now demand that all computers must also have their own defence-in-depth mechanisms such as anti-virus software and personal firewalls, regardless if they are behind a firewall or not. But the controls world has been largely devoid of personal firewall or encryption protection around products such as PLCs, DCS, HMIs and RTUs. As a result, most critical industrial devices have not been as well secured as the average receptionist's PC!

A software-configurable approach in hardware places a firewall security around individual devices – or groups of devices – imparting security isolation down to device level. Eric Byers and Ian Verhappen have led the development effort for the device they call *Tofino*. While both are slightly cagey (***Frank Ogden** writes*) about its precise operational mechanism – for intellectual property reasons the authors say – they make the claim that the hardware can be installed in the field by staff with no security training at all while at the same time permitting company security experts and control system specialists to monitor and manage control system security confidentially from anywhere in the world.

To elicit rather more on what it is and how it works, *The Industrial Ethernet Book* put a few questions to Eric and Ian about their new security technology.

● *Where does this unit sit on the network?*

"The unit is suitable for Zone 2 and can, in fact should be, mounted in the field. It is designed to go where ever the controller (PLC, DCS, etc) is located. For example, if you have a cabinet with a PLC mounted in it you would mount it beside the PLC. We are currently in discussions with several controls vendors to create versions that will mount on their backplanes but these won't be released until early 2008. I should also note it is like a PLC in terms of environmental hardening so it is not waterproof.

● *Does it implement a firewall at fieldbus level as in... unsecured fieldbus commands in, sanitised fieldbus commands out or does it work at a higher (Ethernet protocol) level?*

"It works at the fieldbus level as well as higher levels, with specific field level protocols being supported. The first version has Modbus support with additional buses under development for future release.

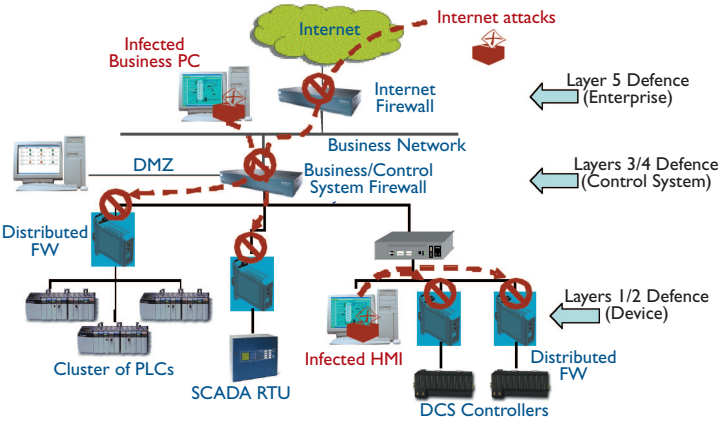
The current version is either serial- or Ethernet-based with support for protocols like Modbus that operate over these common lower layer protocols. This choice was made for two reasons. First nearly every fieldbus protocol now comes in an Ethernet version, e.g. Profinet, FF HSE, EtherNet/IP and so on. Secondly, Ethernet or serial are where most of the serious hacker risk presently is. Further releases will support for speciality physical layers like DeviceNet or FF H1.

Defence in depth for fieldbus…

● *Does the unit implement the firewall action in silicon or software?*
"It is all done in software as downloadable modules much like Function Blocks for Fieldbus. We are able to add new modules 'on the fly' without affecting the operation of existing units.

● What of the update service? How much does a subscription cost... who writes and distributes the updates?
"Updates will be on a subscription basis though we do not yet have the price structure confirmed. The updates will be distributed by MTL after joint development with Byres Security.

● Does the firewall process – whatever it is – affect overall system latency and determinism? – important for motion applications?
"Only in a very minor way, similar to the latency that a typical Ethernet switch might add. We have done extensive testing of this to make sure these delays are acceptable for all processes we have encountered. And a future loadable module is planned that will actually improve network determinism by providing QoS options that one might find in high end managed switches.

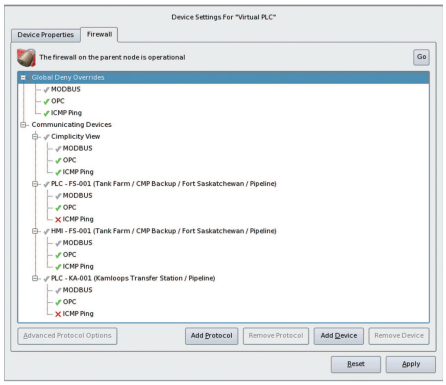


A multilayer defence-in-depth architecture recognises that any threat may be able to bypass any single point of defence but is unlikely to be able to bypass multiple defence points. It also acknowledges the fact that that threats can originate from both outside and within the system. In this illustration we see a control system that is protected by three layers of defence; a corporate firewall to protect the overall enterprise against general internet threats, a business to control system firewall with DMZ to protect the overall control system, and distributed security appliances to protect key assets like PLCs or DCS. The layer numbers correspond to the model of a typical industrial enterprise as defined in the ISA SP-99 Standard for Automation and Control System Security-Part 1.

● *So how do you implement this field-level security system?*
"In a nutshell, we envisage the following… Actually it is what our beta clients have told us they will do.

The control system engineers decide which devices are either vulnerable or mission-critical to their production and safety and thus need defence-in-depth protection based the CERN testing – and that includes most controllers in use today. [*CERN tests reveal IE security flaws; IEB p12, Nov 2006*]

The control system or security staff next set up a Central Management Platform (CMP) somewhere in the company for configuration and monitoring of the Tofino appliances – similar to a configuration station for Fieldbus, but is also remotely accessible using a secure web browser. It can be located in the plant directly on the control system network, in the plant on the business network, at HQ on the enterprise network or all of the above. You



CMP set up screen for configuration and monitoring of the Tofino appliances

can have multiple CMPs to manage and monitor the system.

Technicians are sent into the field to install the units in front of one or more of the identified critical control devices – a single Tofino can protect up to 12 devices. This can be done without impact to the process either before, during or after the CPM is set up. The units just sit quietly waiting for their 'master' CPM to show up and tell them to go into protect mode. While they are waiting, they are in learning mode, completely transparent to the network, yet learning about what is talking to their future protected devices (and how) so the firewall rules can be automatically built.

Once the Tofinos and the CPM are operational, they set up highly secure connections and report what they have learned. The CPM then looks up protection recipes (i.e. templates) for the devices needing protection and suggestion these to the controls technician in charge of the security. The controls tech can then decide to accept these suggestions or edit them using a simple screen with check boxes. (*See screen dump above*).

So imagine you have a system that has a number of AB ControlLogix PLCs that are running a gas turbine. Tofino first discovers what is down stream and needs protection, which in this case, are the ControlLogix PLCs. Next it blocks all traffic that CERN or I will tell you should never be seen near a ControlLogix… If you are suicidal you can over ride these blocking rules. It then tells you what traffic is going to and from the ControlLogix gas turbine controls (and from where) in a simple tree format. You decide what might not be valid traffic by putting a red 'X' in front of those devices you want blocked and a green check mark in front of devices and protocols you want to talk to your PLCs. This replaces the scripting of ugly access control lists like:

```
acl 201 permit tcp any eq 80 10.20.30.0
0.0.0.255 gt 1023 established
```

or…

```
$IPT -A PCN_DMZ -p tcp --dport !
$DH_PORT -j LOG_PCN_DMZ
```

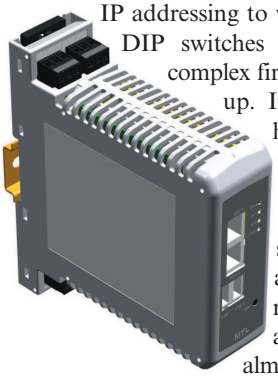
which I can assure you everyone messes up, even if you have been writing these for years!

Next you can safely do a trial run of blocking traffic in Test mode without affecting your process. This is because in Test mode all the traffic still gets allowed through the unit, but you get told what device would not have gotten its message to the PLCs if the Tofino were in full Protect mode.

Finally you can go into Protect mode and see how control system performs with full security operational. If you are concerned at any point you can back out and go back to what was working earlier (just like online programming on an AB PLC).

So the controls tech in charge of security still has to learn what talks to what in the control system and most techs and engineers know that (or at least I hope they do). What they don't know are port numbers, IP addresses, TCP flags, subnets and the like. And in case they don't now what talks to what on their control system, they will get that information presented in tree form so they can make their decisions by checking off a few boxes.

Unlike a traditional IT firewall, there is no IP addressing to worry about, no DIP switches to set and no complex firewall rules to set up. Interestingly this has some import fringe benefits from a security point of view – since the security appliance does not have an IP address, it is almost impossible to detect using common hacking tools. If it cannot be found, it cannot be attacked.



● *Odd name, 'Tofino'?*

"Tofino was originally conceived in my lab at BCIT as a student thesis project about five years ago. At the time we gave the students a small processor called the Surf Board for development. Based on this, the students decided to name the entire project Tofino after the surfer's paradise community on the West Coast of Vancouver Island. As Ian says, we thought the name was catchy and so it has stuck.

Eric Byres *is CEO, Byres Security, Inc.*

Ian Verhappen *is Director of Industrial Networking Technologies, MTL, Inc.*