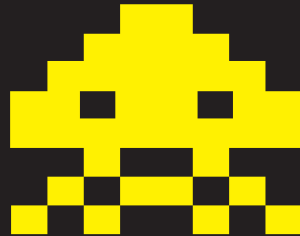
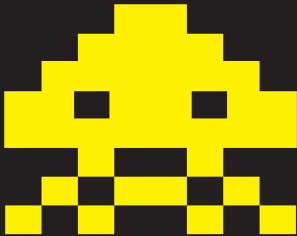


CYBER WARS



KEVIN STAGGS, HONEYWELL ACS ADVANCED TECHNOLOGY LABS, USA, AND ERIC BYRES, BYRES SECURITY INC., CANADA, DISCUSS THE IMPORTANCE OF CYBER SECURITY.



Every month security researchers discover hundreds of new worms and viruses attacking the world's computer systems. Usually, few in supervisory control and data acquisition (SCADA) and process control take notice. In early July 2010, however, a new type of computer worm was discovered that shocked experts in the industrial automation community. Called Stuxnet, this worm had been designed specifically to attack the Siemens WinCC, PCS7 and STEP7 control systems. Suddenly industrial control systems had moved from an accidental target to the centre of the bullseye.

Of course, in one sense this should be no surprise. Security personnel in the US have been warning of the potential for a cyber attack to be its next Pearl Harbour for years. Richard Clarke, the chief counterterrorism adviser to Clinton at the time, raised the prospect over a decade ago, and the comparison has proved enduring; this year alone CIA Director Leon Panetta and Admiral Dennis Blair, the former Director of National Intelligence, have echoed him, and Clarke himself has also been back with his book 'Cyber Wars: The Next Threat to National Security'.

He paints a catastrophic scenario. The 'electronic Pearl Harbour' would start with the collapse of the Pentagon's computer network, followed by a meltdown

of internet service providers. Blows to the power grid, refinery fires and toxic releases at chemical plants would all follow.

Many have rejected this scenario as fanciful, but Stuxnet shows there is cause for concern. Even without a cyber war, it is estimated that there are 400 - 500 cyber security incidents in Fortune500 companies in the US alone each year, and in Europe it is probably worse. In the processing industries and infrastructure, the Repository of Industrial Security Incidents (RISI), which records cyber security incidents directly affecting SCADA and process control systems, shows the number of incidents increasing by approximately 20% a year over the last decade.

For all that though, the truth is probably that the next cyber security incident is more likely to call to mind the Titanic than the Second World War.

In the case of the Titanic an unforeseen accident sunk the vessel, in part because its bulkheads only extended 10 ft above the waterline and failed to make compartments fully watertight. Water from damaged compartments was able to flood undamaged ones, dragging the 'unsinkable' ship down.

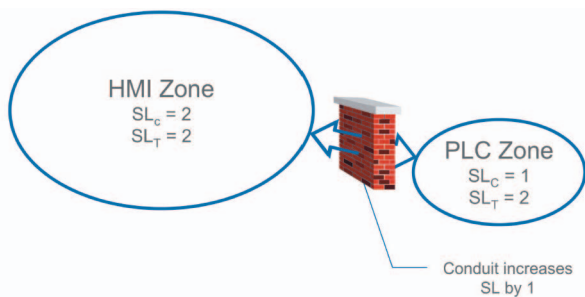


Figure 1. Saving money with zones and conduits. Separate the PLCs and Human Machine Interface servers into their own zones and focus on securing each zone with a conduit.

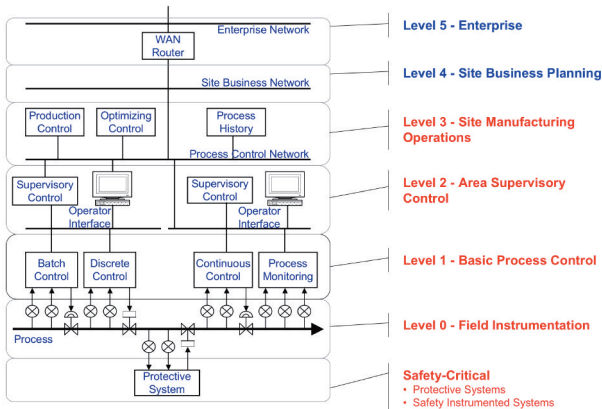


Figure 2. The traditional hierarchical model.

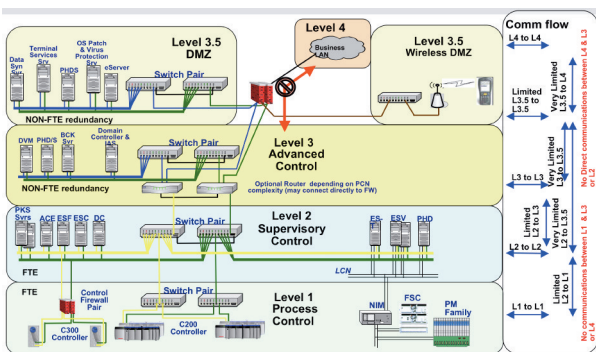


Figure 3. High security network architecture.

It is an apt illustration for most cyber security failures. Consider some examples: the Zotob worm that shutdown 13 assembly lines at Daimler Chrysler in 2005; Browns Ferry nuclear plant in 2006, where redundant drives controlling the recirculating water system failed, probably due to excessive traffic between two different vendors' products on the control system network; or the Hatch Nuclear power plant near Baxley, Georgia, which was forced into an emergency shutdown after a software update to a computer on the plant's business network.

They provide some important lessons for cyber security:

- ▶ Hackers are not the biggest risk. There are numerous other examples of intentional attacks like Stuxnet. In Queensland, Australia, for example, the Maroochy Shire sewage spill in 2000 was the result of a deliberate attack on the SCADA system by a disgruntled applicant turned down for a job with local government. However, such cases remain the minority. RISI figures show that less than a quarter are intentional attacks. Instead, almost 50% of incidents reported have been caused by malware, including viruses, worms and Trojans, not specifically targeted at the facility affected. Many of the remainder are pure accidents. The most common security incident remains the unintended consequence.
- ▶ Internet security is not enough. Daimler Chrysler had professionally installed firewalls between the internet and the company's network, but the worm still made its way into the control system, probably from a laptop. From there it was able to travel from plant to plant in seconds. Or consider the 2008 attack on the Lodz city tram network in Poland. A 14 year old boy used a modified television remote control to change track points, derailing four trams. Any protection of the central control system against untrusted networks was rendered entirely redundant. The hacker was not even using a computer, much less the internet.
- ▶ Poor systems design and, in particular, a failure to contain communications in appropriate areas or subsystems is a key problem. This is perhaps most obvious in the Hatch nuclear example. The safety system there was well designed, right down in the nuclear reactor. Understandably, it included a database to monitor cooling water levels, among other variables. However, it also included a direct link to a similar database in the business network, and unfortunately the data flowed both ways. The result was that when software in the business system was upgraded, zeroing the database there, it did the same to the database in the reactor. The automated safety system interpreted this as a drop in water cooling levels and triggered a shutdown. The plant was offline for two days.

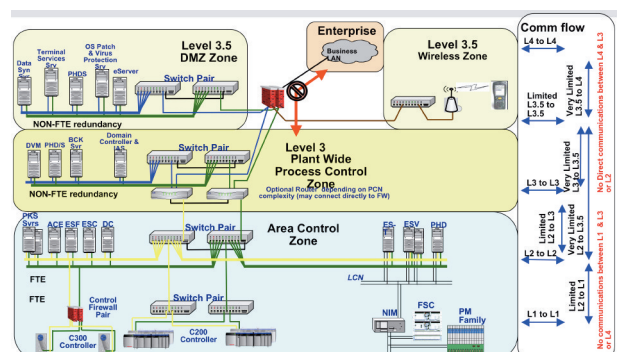


Figure 4. Network architecture as zones.

Defining zones

Behind all of this, of course, is the move away from proprietary networks in process control and SCADA systems to standard platforms, such as Windows and Linux, and open standards such as Ethernet, TCP/IP and web technologies. The benefit this has brought to process control systems is significant; integrating different vendors' technology used to be a significant project, both financially and in terms of time. It can now be a morning's work. Similarly, few would now forego the business benefits of integration with enterprise and third party networks.

However, it has also introduced vulnerabilities. Control systems can no longer rely on security through obscurity. Instead, they need the same protection against network attacks and vulnerabilities that have long plagued enterprise IT systems.

Unfortunately, perfect security is unachievable and, even if it were, would be unaffordable. What is required therefore is network security that protects against external threats, while preventing problems that do materialise in one part of the system spreading to other critical control systems. The solution is security zones.

Based on the ANSI/ISA 99 and (soon to be ratified) IEC 62443 standards, key automation and control devices should be grouped into zones that share common security level requirements. Any communication between these zones must then pass through a conduit, a path that regulates the flow of data between zones to allow them to communicate securely.

Defining the security level of each zone is not easy. At a minimum, ISA 99 requires three levels for security zones: high, medium and low. Each zone will require a security level target (SL_T), based on a risk analysis of the plant, taking into account the consequences and likelihood of the range of possible threats. Equipment in each zone will have a security level capability (SL_C). If this is lower than the SL_T value, a security technology or policy needs to be added to equalise them.

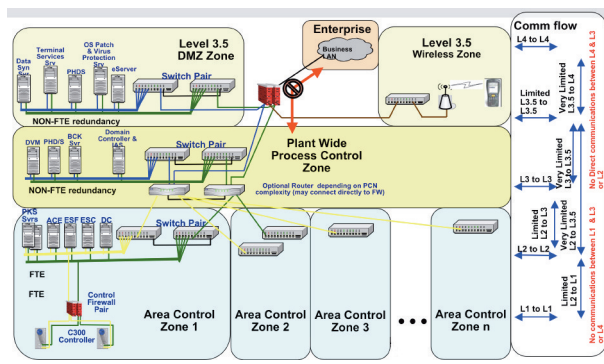


Figure 5. Multiple area control zones.

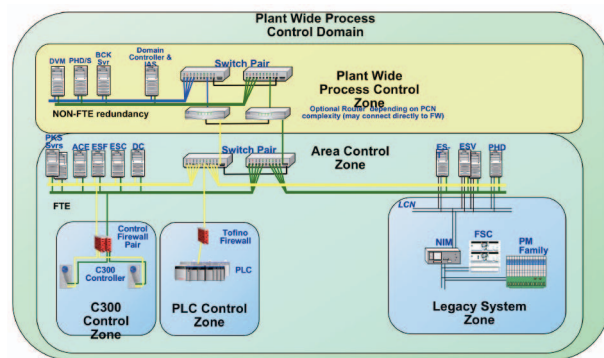


Figure 6. Zones within zones.

Take, for example, Windows XP based HMIs. These typically have an SL_C greater than a group of PLCs or Windows NT servers on a legacy system, which, as obsolete technology that can no longer be kept updated, represent an area of vulnerability. Within the system, however, the HMIs, PLCs and NT servers may require the same security level. The solution is to separate them into separate zones and to use the conduit to increase the security level by one (Figure 1).

This approach has three major advantages:

- ▶ **Cost control:** Securing the whole system to the level needed by the PLCs or NT servers would be prohibitively expensive and, in the case of the servers, not even possible. It would require complex process edge VPNs, firewalls for each device, and possibly wholesale replacement. Using security zones, technology to increase the security level is only added where the SL_T , which is based on the actual risk posed, requires it.
- ▶ **Detection:** Poor segmentation makes it difficult to locate the origin of any problem that does materialise. Zones aid with this identification, enabling operators to resolve it at the source and pinpoint vulnerabilities.
- ▶ **Containment:** A properly compartmentalised network in which traffic only passes between zones where necessary, and then only through defined and appropriately secured conduits, will prevent problems spreading and protect mission critical control systems. In fact, mechanisms should be in place not only at the zone's border but within it, to stop problems spreading from device to device even within zones. In effect it is possible to create zones within zones. Together these zones form an essential part of a defence in depth, multi layered security system.

Network architecture

These principles can be seen worked out in the system designs. Figure 2 shows the traditional Purdue hierarchical model, which formed the basis for ISA 95, the international standard for the integration of enterprise and control systems. A layered network topology with the most critical systems deeper within it, it provides multiple levels of protection.

At Level 0 in the control system are the sensors and valves. Level 1 works in both the control system and a SCADA environment, and is where the controllers tie in (the PLCs, DCSS and PID controllers and so on). At Level 2 the HMIs come in, enabling modifications to be made to the process. Level 3 is the site wide or plant wide control. The key break is between this level and those above it. On Level 4 the MES systems start to come into play, and one is into an IT environment, with significantly different security priorities.

Figure 3 shows Honeywell's implementation of this. Components and data are compartmentalised and network traffic is limited to necessary communications. A firewall between Level 3 and 4 creates a logical break between the enterprise network and the process control network. As shown on the right of the diagram, there are no direct communications between Level 4 and 3 or Level 2. A demilitarised zone (DMZ) at Level 3.5 houses the servers for where data needs to traverse from the process system to the business systems. It is also a good place to put the management servers, and therefore contains an operating system patch manager and an antivirus server. Figure 4 shows this architecture in terms of zones, where Level 1 and 2 are treated as a single zone.

In Figure 5 this is applied to a typical plant in which operators control multiple areas. The design includes multiple area control zones to allow the operator to maintain control of the different areas in the event of an incident affecting the plant wide control network. Even if its connections are broken, the plant can still be

operated at lower levels, although functions such as plant wide control and optimisation will be lost.

Finally, Figure 6 shows how security is increased using zones within zones. The PLCs, for example, typically communicate with the control system through the Modbus Protocol over TCP/IP, which communicates through a single port. Therefore, no other ports need to be open between the PLC and the control system. At the same time, the PLC configuration station on that network needs greater communication with the PLCs. However, there is no reason for it to communicate with the Experion PKS. That is why the Tofino firewall is in place. This keeps any traffic between the PLCs and their configuration station local to the PLC network, with only the Modbus traffic allowed to flow across.

This is particularly important since most devices on Level 1, such as the PLCs, are embedded systems, with limited resources; for example due to memory constraints, there often a very limited number of buffers with which to communicate with the network. If the network experiences a spike in traffic, as from a denial of

service attack, the network buffers of PLCs can easily be filled. The firewalls help prevent that from happening.

Making a start

The most obvious objection to implementing security zones is the upfront work involved, particularly when it comes to existing plant networks, and that is just one reason that the process should start with a thorough risk analysis. An extract from such a risk analysis is shown in Table 1. This will clarify and, where possible, quantify the business consequences should the threats identified materialise. These may be in terms of lost production, repair costs, cleanup costs or fines, not to mention environmental damage and loss of life. Identifying the potential to incur these costs will be key to defining the business rationale for implementing a robust cyber security system and gaining management support for it.

Furthermore, a risk analysis focused on the operational zone will help clarify the distinction between the threats facing the control system against those more commonly considered in the IT environment. This is vital because much of the knowledge needed for

the exercise will come from the company's IT department, which will have the expertise in server and fire wall management, disaster recovery, backup and restore procedures, and so on. It makes sense to make use of this. Control systems are, after all, similar to mission critical servers in the IT space.

However, the priorities in the control room are not the same. IT personnel are primarily focused on protecting the company's intellectual property; process control security is about protecting the physical assets, the plant, its people and the surrounding environment. Similarly, patch management, firewalls, antivirus software and encryption must all be handled radically differently in a control environment. The analysis will help highlight these differences.


Finally, a risk assessment should help reveal the vulnerabilities that are actually in the system. It will, for instance, necessarily involve an inventory of the networks that will reveal where design drawings may no longer be up to date, and should help to determine where the risks actually lie. This will prevent any security strategy focusing just on high profile, but low probability events, such as a terrorist attack. Instead, the whole range of everyday threats can be identified, revealing the close interconnection between security, safety and reliability. The plant can then prioritise dealing with the high probability, high impact vulnerabilities. That, in turn, should leave it as well placed as possible even if Clarke's worst fears do turn out to be true. 

Table 1. A risk analysis of the operational zone

Threat	Vulnerability	Possible threat source	Skill level	Potential consequence	Severity	Likelihood	Risk
Release of hazardous product	Manipulate control system	Organised crime, activist	Intermediate	Major injury complaints or local community impact	Medium	Low	Low risk
	Disable/manipulate emergency shutdown	Terrorist, organised crime, activist	High	Fatality or major community incident	High	Very low	Low risk
Process reactivity incident	Manipulate control system	Domestic or foreign terrorist, disgruntled employee	Intermediate	Lost workday or major injury complaints or local community impact	Medium	Low	Low risk
	Disable/manipulate emergency shutdown	Domestic or foreign terrorist	High	Fatality or major community incident	High	Very low	Low risk
Process shutdown	Trip emergency shutdown	Malware, novice hacker	Low	Shutdown > 6 hrs	Medium	High	High risk
	Cause loss of view of SIS	Malware, novice hacker	Low	Shutdown > 6 hrs	Medium	High	High risk
	Manipulate control system	Hacker, disgruntled employee	Intermediate	Shutdown > 6 hrs	Medium	Medium	Medium risk
	Disable PCN communications	Malware, novice hacker	Low	Shutdown > 6 hrs	Low	High	Medium risk
	Spoof operators	Hacker, disgruntled employee	Intermediate	Shutdown > 6 hrs	Low	Medium	Low risk
Environmental spill	Manipulate control system	Activist	Intermediate	Citation by local agency	Medium	Low	Low risk
	Mislead operators	Activist	Intermediate	Citation by local agency	Medium	Low	Low risk