Certitude
TECHNOLOGY RISK SERVICES

- 3 / 480 Collins Streeet
  Melbourne Vic 3000
- +61 (0)3 8610 6700
- www.certitude.au.com

Common SCADA & Process Control System Security Myths

Eric Keser
Director
Certitude Pty Ltd

When I was studying applied physics at university my lab partner and I designed and built an anemometer (a device for measuring fluid flow e.g. wind speed) that had no moving parts what-so-ever. The anemometer was electronic and connected to a Commodore 64 computer (not to show my age) which collected data from the device, performed several complex calculations, and displayed the speed of the fluid being measured. Little did I realise at that time that we had essentially built a mini Supervisory Control And Data Acquisition (SCADA) system. What strikes me today is the overwhelming lack of consideration for security we designed into the system at the time. Our focus was purely on building a system that was industrially functional and reliable.

While our little anemometer system was nothing like the complexity and extensiveness of real SCADA and Process Control Systems (PCSs) used today, in the past the same mind-set prevailed with regard to designing and building security into even the large and complex systems. And while there has been much discussion and progress made in addressing this issue, there are still many inherent problems which make the retrofitting of security difficult to PCS/SCADA systems. Along the way, several myths have formed concerning PCS/SCADA security which warrant some discussion.

What are PCS and SCADA Systems?

Before we discuss these myths, it is important that we spend some time discussing the nature of these systems. In particular, it is important to acknowledge some of the fundamental differences between these systems and other more general IT systems.

PCS/SCADA systems are used in industries such as manufacturing, mining and raw material processing, and utilities (e.g. water, electricity, and gas) to automate and manage infrastructure such as valves and pumps, circuit switches, wine making tanks, speciality systems such as life support systems for remote outposts (e.g. bases in Antarctica), and physical security systems (e.g. CCTV, door switches, fire detectors and alarms etc).

- 3 / 480 Collins Streeet
  Melbourne Vic 3000
- +61 (0)3 8610 6700
- www.certitude.au.com

The systems normally perform a number of the functions related to the assets they are deployed for. These functions however can normally be reduced to three basic categories:

- **Control** (e.g. changing operating ranges/settings/levels, starting/stopping pumps, opening/closing switches, unlocking/locking doors);
- **Monitoring** (e.g. data collection and archival, data trend analysis, long-term asset planning, management/regulatory reporting); and
- **Alarms & Alerts** (e.g. pump failure, blackouts, water/sewages overflow, and doors left opened). Alarms and alerts may be triggered by the occurrence of a single event, or at a more intelligent/intuitive level following a series of specific consecutive events).

Initially PCS/SCADA systems were essentially isolated systems with a fair amount of mystic surrounding them due to their specialised and often proprietary technologies. However, over the years these systems have become more vulnerable to attack, mostly due to:

- Increased use of public telecommunications networks (e.g. Internet, CDMA and GSM) rather than private networks such as leased telephone lines;
- Increased migration from proprietary standards and protocols, to common and open standards and protocols; and
- Increased connectivity and functionality of PCS/SCADA networks to corporate, business and joint venture partners, vendor, third-party operator, and maintenance and support provider networks.

While the systems are becoming more exposed to security incidents, primarily due to the above, there are a number of PCS/SCADA system idiosyncrasies which make it difficult to impose traditional IT security practices on them. These include, but are not limited to:

- Needing to operate in real-time and continuously with very little or no downtime;
- Having little or no built-in security functionality and capability;
- Having limited vendor support for upgrades, and as a consequence often operating on un-supported operating systems and un-fixed vulnerabilities; and
- A lack of adequate testing environments.

The combination of the previously mentioned changes to the PCS/SCADA systems and their specific idiosyncrasies certainly increase their vulnerability to security incidents. However the level of actual impact a specific security incident causes is dependent on:

- The value of the affected asset(s) to the organisation;
- The level of dependency, sophistication, and positioning within the system of control provided by the PCS/SCADA system; and

3 / 480 Collins Streeet
Melbourne Vic 3000
+61 (0)3 8610 6700
www.certitude.au.com

- The level of dependency on monitoring and reporting provided by the PCS/SCADA system.

MYTH 1 – Redundancy Takes Care of Everything

PCS/SCADA systems typically are designed and deployed with a high level of redundancy in the form of alternative network links, and duplication of Input/Output and terminal servers, (Programmable Logic Controllers (PLC)s, power supply, and Human-Machine Interfaces (HMIs). This level of redundancy offers protection from limited local failures, but does not address whole-of-site failures. The later can normally only be addressed by comprehensive Business Continuity Planning (BCP) and IT Disaster Recovery Planning (DRP) yet these are often overlooked with comfort justified by the level of redundancy alone.

While some organisations may recognise the importance of DRP, there are also legitimate reasons for not having a DRP for particular sites. For example, it may not make sense to plan for a whole-of-site SCADA loss if the cause of the loss is likely also to cause the loss of the assets at the site which the affected system is managing.

There are also legitimate reasons for not having a BCP in place, but instead relying heavily on a robust and comprehensive DRP. For example, many organisations have reduced the number of operating staff and their skills and experience (perhaps as an outcome of PCS/SCADA deployment) to a level such that there would be no practicable way to cover all the affected assets manually given an extensive system loss.

MYTH 2 – PCS/SCADA Systems Need to Remain Isolated

We saw previously that there has been an increasing level of interconnectivity between PCS/SCADA systems to other networks. The main reason for this has been to derive the business benefits of greater inter-business and trans-organisational collaboration.

In order to keep the usefulness and value of PCS/SCADA systems in today's world, it is inevitable that they will be increasingly interconnected to other networks, some of which the owner of the PCS/SCADA systems does not control. As an example, I recently worked with a major global mining company who had many PCS/SCADA systems located around the world. Forced by a need for greater collaboration across the company their PCS/SCADA systems were increasingly being interconnected to other networks. What originally resulted as a consequence of the push towards greater collaboration was a mind set that the company's entire global network was to be treated as one large trusted network. In other words, any individual system could essentially trust any other system on the company's network. It soon became apparent through a risk assessment process that in fact the PCS/SCADA systems had a very different level of importance that needed to be acknowledged and therefore treated differently from other systems on their network.

3 / 480 Collins Streeet
Melbourne Vic 3000
+61 (0)3 8610 6700
www.certitude.au.com

A way had to be found to allow the connectivity (and collaboration), yet provide the high level of protection required by the PCS/SCADA systems.

MYTH 3 – Normal IT Processes Are Suitable

IT professionals have over the years established a series of good practices concerned with managing general IT environments. However for the most part, these practices have developed outside the specific operational needs and limitations of PCS/SCADA systems, thereby lacking alternate mechanisms to address some fundamental PCS/SCADA security issues. This has become a little bit of a problem because in recognising the need to impose better system management practices over PCS/SCADA systems, many organisations are migrating their management from their traditional engineering departments to their IT departments.

For the most part these processes relate to making changes to PCS/SCADA systems which are problematic due to restricted available time to make such changes, a prevailing "if it's not broken don't try to fix it" attitude, and sometimes a lack of vendor support for the intended changes. These changes include:

- Applying security patches to remove known security vulnerabilities; and
- Upgrading operating systems.

In additional to the above, good IT security practice prescribes the notion of authentication and authorisation (the mechanisms of proving who you are, and what you are allowed to do). Unfortunately, many PCS/SCADA technologies lack the capacity and the capability to have such mechanisms deployed at all the required levels of the system. The Maroochy Water Services security incident a few years ago demonstrated how systems lacking such mechanisms are vulnerable to attack. The good news is that PCS/SCADA system vendors are beginning to provide these capabilities, and move to non-proprietary standards and protocols which will allow authentication and authorisation mechanisms to be deployed in the future.

MYTH 4 – Proprietary Operating Systems Are Less Secure than Open Systems

This is a commonly raised debate in the PCS/SCADA and IT security community. Without bias, the reality is all software, and even hardware, has potential errors which can be exploited to breach security. It's the same outcome whether it's an open system or a proprietary one.

For augments sake, let's look at the facts surrounding the hotly debated Windows versus UNIX operating systems. On the UNIX side it can be argued that it is inherently more security due to the fact that the programming code is openly published for wide public scrutiny and that its been inherently designed with better security from the start. It can

3 / 480 Collins Streeet
Melbourne Vic 3000
+61 (0)3 8610 6700
www.certitude.au.com

also be argued that, due to the targeted focus on finding Windows vulnerabilities along with the wider deployment of Windows environments, Windows has in the end been more thoroughly subjected to focused scrutiny. It is also true that while Windows source code is not publicly published for open scrutiny, it is published to certain government agencies for their scrutiny.

In any case, no matter what the technology deployed, each will inherently have its errors and it only takes one error to be exploited to cause impact. No matter which technology used, from a security point of view you will always need to:

- Determine your specific security requirements based on the value of, and impact on, the asset(s) you wish to protect;
- Select the technologies that provides the level of security functionality and support that meets your requirements;
- Test the technology to ensure it meets your requirements; and
- Most importantly, maintain the technology e.g. patch, upgrade, assess, employ layers of security, adopt good procedures etc.

MYTH 5 – All Systems Are Alike

Attacking PCS/SCADA systems is not unlike attacking traditional IT systems. However there are often added obstacles to an affective and targeted attack which, even today, prevail over PCS/SCADA systems. These include such things as:

- The existence of manual controls which can override PCS/SCADA controls;
- The need to have some level of PCS/SCADA operator knowledge to have specific intended attack results, such as a sewerage spill;
- The need to know how to bypass alerts and alarms in order to prevent detection;
- The need to often have some level of initial PCS/SCADA operator access and/or connectivity to the PCS/SCADA system; and
- In some cases, the need to have some knowledge of PCS/SCADA proprietary protocols.

If we keep the above in mind and we also consider the types of security attacks and the types of attackers, we begin to build an initial risk profile of a typical PCS/SCADA system.

For simplicity, let's discuss security attacks in terms of confidentiality, integrity and availability, and discuss attackers in terms of insiders (employees, contractors, third-party operating and support providers), and outsiders (e.g. the general public).

In doing so, a typical attack profile for PCS/SCADA systems may look something like that in the table below.

3 / 480 Collins Streeet
Melbourne Vic 3000
+61 (0)3 8610 6700
www.certitude.au.com

	Loss of Confidentiality	Loss of Integrity	Loss of Availability
Outsider	Low	Medium	High
Insider	Medium	High	Medium

Table 1 – Overall Risk of Typical PCS/SCADA Attack

If we take each attack type in turn, for most PCS/SCADA systems the need to protect the system's confidentiality not normally high, as there is often little secret information stored and processed by such systems. Therefore, an attack which results in the loss of confidentiality may be a lower risk than an attack of one of the two remaining types (integrity and availability). It is also less likely that if there is secret information in the PCS/SCADA system, an outsider is less likely to know about it and to appreciate its value than an insider would. Hence, the risk profile concerning loss of confidentiality is low for an outsider and slightly higher for an insider.

In the case of loss of integrity, the over-riding contributors to the level of risk are primarily the importance of being able to control the asset(s) and the level of dependency on the PCS/SCADA system for such control. And once again, an insider would have a much better understanding of what specific outcomes are caused by altering the way the system behaves than an outsider. This is the type of intended attack that an insider is more likely to focus on, as was the case of the Maroochy Shire Water sewerage spill.

Conversely, given they usually lack the knowledge of PCS/SCADA system operation, an outsider is more likely to cause a loss of availability. This can be done without any knowledge of the system and provoked by simple trial and error to cause an unintended result, or by employing known techniques for system denial of service attacks. In addition, we can treat viruses and worms essentially as outsiders and which typically cause system unavailability or performance degradation without PCS/SCADA system knowledge.

The well publicised Maroochy Water Services sewerage spillage is a classic example again of the advantages an insider has over an outsider when attacking industrial systems. In the Maroochy case, the attacker was an ex-employee of Hunter Watertech (a supplier to Maroochy Water Services), who was involved in the setup and operation of the Maroochy SCADA system.

The attacker made 46 successful intrusions mostly undetected, until the final acts of causing a spillage were detected by Maroochy staff, demonstrating how an insider's knowledge of system controls, monitoring, alarms and alerts can be used to evade detection.

- 3 / 480 Collins Streeet
  Melbourne Vic 3000
- +61 (0)3 8610 6700
- www.certitude.au.com

Further to this, in order to perform the attack, the attacker knew what equipment he needed to perform a directed attack. For example he:

- Stole a Hunter Watertech laptop which was already configured to communicate with the system.
- Purchased and used commercial radio equipment which he knew he could use to connect to the SCADA system.
- Used control management software to affect the SCADA system in a controlled and deliberate manner.

While there are existing and worthwhile guidance concerning PCS/SCADA security such as from the TISN[1], and other more general IT governance/security guidance such as AN/NZS7799[2] and from ISACA[3], the practicalities of implementing such guidance requires specific awareness and careful consideration for the idiosyncrasies and needs of PCS/SCADA systems. Often such deployment into PCS/SCADA systems is far more difficult than for more general and traditional IT systems. As time goes on it is hoped however that PCS/SCADA systems will eventually evolve to make the deployment of much needed security easier.

Risk management, like art, is all about how you draw the line.

[1] Trusted Information Sharing Network for Critical Infrastructure Protection (www.tisn.gov.au)
[2] www.standards.com.au
[3] www.isaca.org