The number of incidents involving attempted unauthorised access to computer systems via the internet as reported by CERT (Computer Emergency Response Team) was 137,539 in 2003. Statistics show an exponential increase in the number of reported incidents in the last five years. Although this can be partly explained by the increase in the number of computer systems in the world that are connected to the internet, it is nevertheless an alarming fact.

white paper

SCADA Security

threats to SCADA systems

Potential threats to SCADA systems come from a variety of sources including commercial rivals, ex-employees, hackers and script kiddies, terrorists and malware such as viruses, trojans and worms. A number of high profile incidents involving control systems, such as the Slammer worm's intrusion into Davis-Besse Ohio nuclear power plant network have unfortunately given SCADA systems bad publicity. Not only has this publicity painted the current security of these systems in a negative light, but it also publicises their very existence. Whereas in the past a SCADA system could be said to operate with a sense of "security by obscurity", it is no longer the case that they can be considered invisible to the outside world.

designing for security

Prevention, detection and recovery are the key points for dealing with a security incident. These points should be considered individually at the system design phase to assess how they can be incorporated into the system and what impact these measures will have on its operation.

preventative measures

The Prevention is the process of reducing the risk of a security incident. The majority of effective, preventative measures require that they be built into the system design and architecture and not added on later. Prevention should also be part of regular system maintenance activities.

> page 2

Examples of preventative measures are:

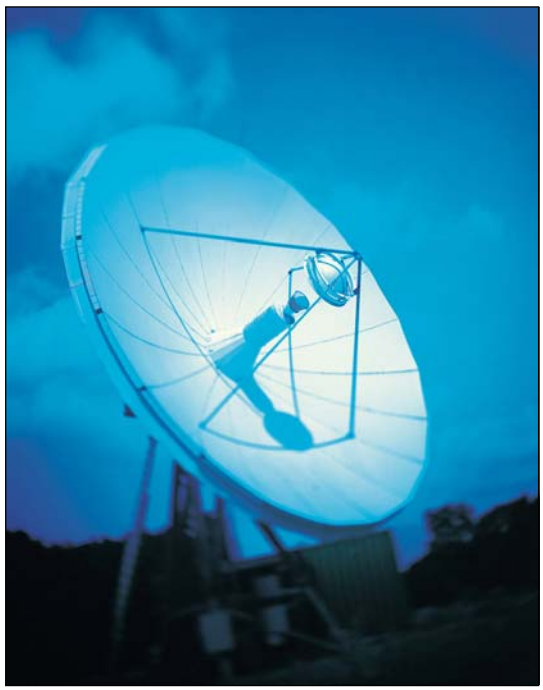
- Separate SCADA and corporate networks
- Installing latest security patches for both software and operating system
- Data encryption
- Configuring firewalls
- Virus scanning
- Configuring user authorisation and permissions
- Strong passwords
- Use of keycards or badges
- Limiting availability of (technical) information about the system
- Securing the operating system by removing default accounts and closing unused ports and services
- Special attention to potential backdoors in the system, such as service related dial-in lines

detection methods

Detection is the ability to recognise a security incident should it occur. This usually involves activating logging and recording features at various levels, and regularly examining them. It is important to maintain a good balance with the amount of data being collected. Too much information will make detection difficult and tedious, resulting in important information being overlooked, or that the task becomes so complex that it is ignored.
Another important element of detection is recognising normal behaviour patterns. For example, a shift change will occur at a specific time of day and system operations will leave a natural trail from its day to day activities. It is the deviations to this regular pattern that are of interest when looking for potential security breaches.

Examples of detection methods are:

- Closed-circuit television
- Visitor logs
- System administration tools
- Historical field data
- Security alert mechanisms (hardware and software)
- Audit trails and logs in application software
- Operating system log files



recovery

Recovery is the ability of restoring a compromised system to its operational status. Note that this may involve more than the affected system alone and include other systems to which it interfaces.
NB: The Y2K experience was for many an exercise in disaster recovery and contingency planning. Similar practices need to be employed when considering disaster recovery techniques.

Points to consider with respect to recovery include:

- Fault-tolerant, redundant hardware
- Fallback mechanisms
- Impact assessment of loss or disconnection of one or more system components
- An unambiguous, tested disaster recovery plan
- An unambiguous, tested system backup procedure
- A procedure for reviewing and learning from any security incident

> page 3

segregating your network

A useful way of defining methods for prevention, detection and recovery is by dividing the control system into logical zones. Each zone should be considered a separate, defendable entity. The control network not only links the various supervisory and control system modules but is often connected to the outside world via number of paths. By breaking the system down into sections it is easier to identify user rights at application and operating system level, the vulnerable points in the zone and the means required to harden the zone against attack. The zones of vulnerability can be derived by examining the SCADA network infrastructure architectural designs.

A typical SCADA project contains zones for:

- The corporate network
  Data historians and MES systems are included within the corporate network.
- The service network.
  This zone is used by the service and maintenance personnel of the system vendor. Often accessed via a password protected, dial-back modem connection.
- The field network.
  This includes the PLCs and fieldbus equipment. This part of the network is connected to the supervisory system via RS232 serial lines, Ethernet etc.
- The remote access network or extranet.
  Used by remote or roving operators and site maintenance engineers. This network may be accessed via a VPN or directly via the internet.
- The control network.
  This is where the SCADA system is located which includes the control room operator stations and the data acquisition front-ends for example.

Note that the zones represent logical sections. For example, if there are PCs in the control room that are connected to the corporate network (for email and office related activities), these should be considered part of the corporate network zone and not the control zone.

layers of protection

It is clear that the SCADA network is embedded in a larger scheme. Only providing protection in the outermost zones (e.g. between the internet and the corporate network) means that an attacker only needs to break into the outermost level to gain access to the entire network. In theory every interface between the control zone and another zone provides a potential break-in point and path of attack. For example, the corporate network should be treated as if it was as potentially hostile as a foreign network or an internet connection. This means building a separate level of protection for the control zone, in addition to any protection that exists for the corporate network.

Furthermore, a single zone can be considered as being made up of a number of different layers, each of which can be considered separately These layers include:

- Security policies and procedures
  Definition of rights and privileges to individuals based on job description, visitor logbooks, use of hardware keys, conscious choice of strong passwords, disaster recovery procedures, disconnect dial-back modems when not in use etc.
- Network layer
  Use of IPSec for encrypted IP traffic, removing unnecessary network services, closing default open ports,
- Operating system,
  Passwords at OS level, user and group file and disk permissions, removing or restricting access to unnecessary applications, removing default accounts and changing default passwords, etc.
- SCADA application
  Passwords at application level, audit trailing, process areas, custom scripts and applications etc.
- Proxies
  Perform service requests such as HTTP internet access on behalf of client systems, which are often protected behind a firewall.
- Firewalls
  A machine acting as a gatekeeper that only allows specific traffic to coming in from or going out to another network (often a WAN or the internet).

> page 4

conclusion

The key points for securing network infrastructure against cyber threats are prevention, detection and recovery. The following list summarises the main points of this document with regard to securing a SCADA network.

Examples of detection methods are:

- Define a security policy for the system in which access rights to the various components of the system are identified, methods for preventing, detecting and recovering from a cyber incident are described and an incident response team is defined.
- Treat any network outside the SCADA network as though it was public and secure these connections accordingly. Only allow traffic into the network that needs access to it.
- Design the system in such a way that the SCADA server can be isolated from the corporate network
- Design disaster recovery into the system (e.g. fault-tolerant host, backup procedures including system images, PLC configurations and application configuration files).
- Remove or deactivate any unnecessary network services from the system.
- Keep the system up to date with the current, safe versions of operating system patches, employed network services and virus scanning software.
- Monitor the system behaviour and log files for suspicious or unexpected activity.
- Educate your users. Provide awareness of the value of strong passwords and how to manage them. Both the end-user and incident response team should have sufficient knowledge of the system that they can maintain and secure the system properly. Make sure they are familiar with the security policy and know what to do in the case of an incident.

Yokogawa System Center Europe B.V. ¬ Lange Amerikaweg 55, 7332 BP Apeldoorn / P.O. Box 20020, 7302 HA Apeldoorn, The Netherlands ¬ Tel: +31 (0)55 538 9500 ¬ Fax: +31 (0)55 538 9511 ¬ www.yokogawa.com/eu