PREMIUM PIPELINES INTERNATIONAL digest

Cyber-attack protection for pipeline SCADA systems

by Tobias Walk, ILF Consulting Engineers GmbH, Munich, Germany

Pipeline supervisory control and data acquisition (SCADA) systems form critical IT infrastructure which are becoming more and more susceptible to well-directed cyber attacks. A popular example would be the Stuxnet-Worm which has been specifically developed and distributed to attack modern control systems. In order to protect IT infrastructure against modern cyber attacks, various aspects need to be considered during design as well as during operation and maintenance of these systems. This article provides examples of IT threats within process control systems, and briefly explains the control system components and system architecture that have been developed over the last decade to identify and flag the system's vulnerability.

SCADA systems are used to control and monitor physical processes. They are commonly used within the pipeline industry – particularly for oil and gas transportation but also for electricity transmission, water distribution, and for many other systems in modern society.

SCADA systems provide operators with a transparent, real-time view of a complex process environment via their human-machine interface, which is necessary from process control, operational and integrity points of view. The operator can remotely start, stop and select various plant operation regimes, and prevent critical process conditions based on information gathered and provided by the SCADA system. Customised dynamic process information displays and alarm handling managers support these tasks, and form an integral part of the SCADA system.

SCADA systems are based on communication networks as they interconnect and integrate field equipment – e.g. actuators, process sensors or pumps – via remote terminal units (RTUs) and local station/unit control systems based on programmable logic controllers (PLCs) with the control centre computer system. SCADA systems are required for an efficient management of a remote and widely distributed process, and support the integrity of the pipeline.

A typical SCADA system layout is shown in Figure 1. These days, the process control networks are interconnected with office networks to provide process data to enterprise resource planning (ERP) applications as well as to other third-party networks for data exchange or maintenance purposes.

The evolution of the SCADA system

The use of SCADA systems has become popular since the 1960s as a need arose to more efficiently monitor and control the status of remote equipment. The first-generation SCADA system had

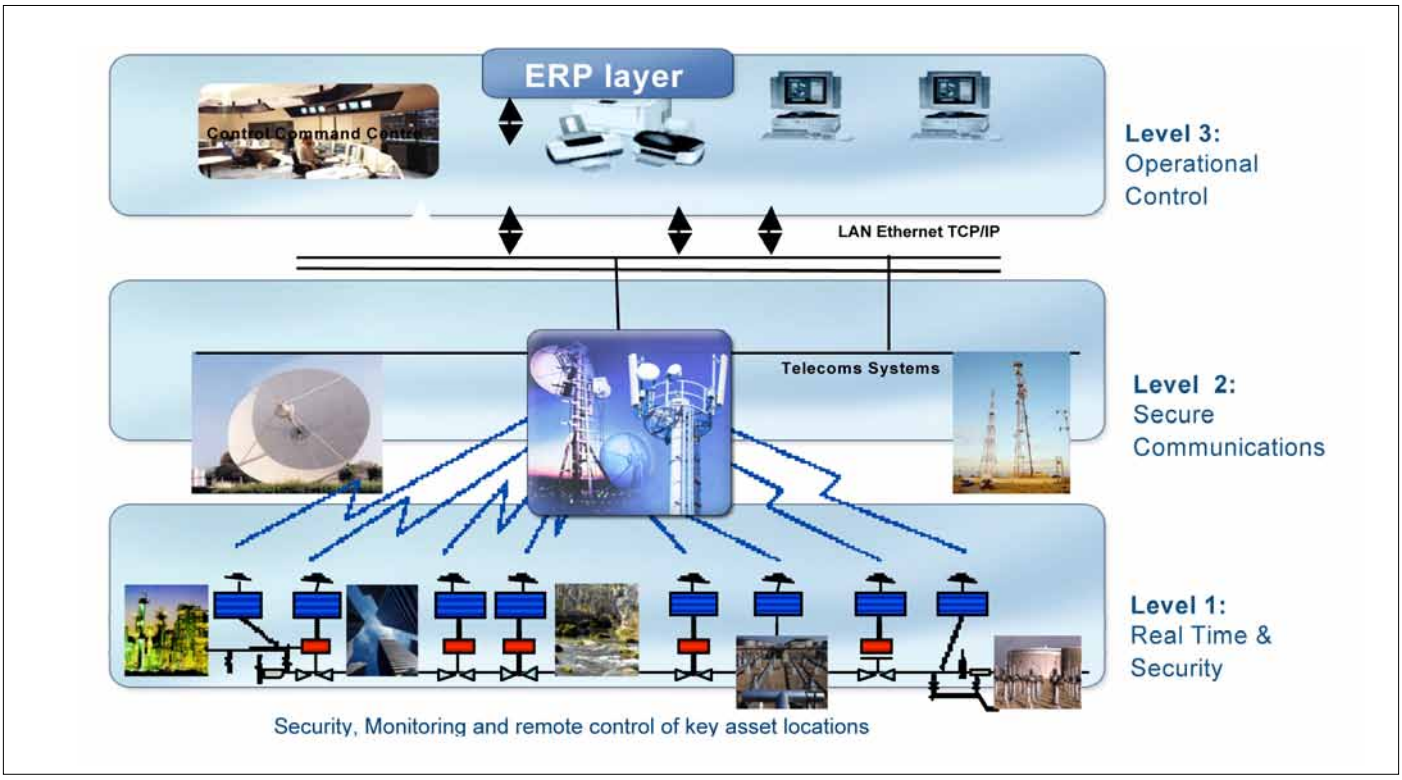

Figure 1: Typical layout of a SCADA system.

'monolithic' system architecture and was based on redundant mainframe computers. These mainframe computers collected all process data from the field and hosted a real-time process database. At that time, computer networks did not exist and communication protocols with RTUs were often of a proprietary type. SCADA systems were independent, stand-alone systems with no connectivity to other systems.

The second-generation SCADA system distributed processing across multiple stations which communicated via a local area network (LAN) in real time with each other. Each station was responsible for its dedicated tasks which significantly reduced the performance, capacity and costs of the required computer hardware compared with the mainframes of the first generation. However, the network protocols utilised were still mostly proprietary and optimised for real-time applications, quick response times and redundancy. As these networks were still being used exclusively by SCADA systems, data security and data encryption was not an issue at the time. Only very few people beyond the developers and hackers knew enough to determine how secure a SCADA installation really was, and they had no interest to flag or discuss the status quo of its security.

The third-generation SCADA system is based on open-system architecture rather than a vendor-controlled proprietary environment. The SCADA system utilises open standards and protocols, thus distributing functionality across a wide area network (WAN) rather than a LAN. It is easier to connect third party peripheral devices, such as printers or hard disks, to open architecture. WAN protocols such as internet protocol (IP) are used for communication between the operator master station and communications equipment.

Due to the use of standard protocols and the fact that many networked SCADA systems are now also accessible from the internet, the systems are potentially vulnerable to remote cyber attacks. On the other hand, the use of standard protocols and security techniques means that standard security improvements are applicable to SCADA systems, assuming they receive timely maintenance and updates.

SCADA systems have been a reality for decades, but over time, market developments have migrated its infrastructure from proprietary, obscure and isolated systems toward standardised, documented and connected systems (see Figure 2).

Conflicting cultures of IT security

While technologies such as ethernet and TCP/IP allow for significant cost savings and improved interfacing for industry, it is important to understand that their origins are derived from a culture very different from the process control provided by SCADA systems. Even a new internet user can spot these differences in terms of reliability; occasional failures are common and tolerated on the internet while most control systems are expected to operate for months, if not years, without interruption. Similarly, the tradition of beta testing many new internet products in the field and recovering from problems by simply rebooting servers or switches contrasts sharply with standard SCADA practices. This is not surprising since the risk impact of outages on the internet are typically loss of data, while outages in the process environment will certainly result in loss of production and may even cause loss of equipment or life.

The internet culture and its created technologies are based on the idea that performance is paramount and outages, while undesirable, are acceptable. This is clearly not true for industrial process control systems. These differences in expectations are briefly summarised within Table 1 and need to be kept in mind when implementing solutions from the internet world within an industrial control environment.

Security issues within SCADA systems

Most companies are reluctant to report cyber attacks or even internal accidents as this can blemish their reputation. Incidents involving health, safety or environmental degradation may even jeopardise their company's license to operate. The British Columbia Institute of Technology (BCIT) maintains an industrial cyber security incident database that tracks incidents involving process control systems in all sectors of manufacturing.

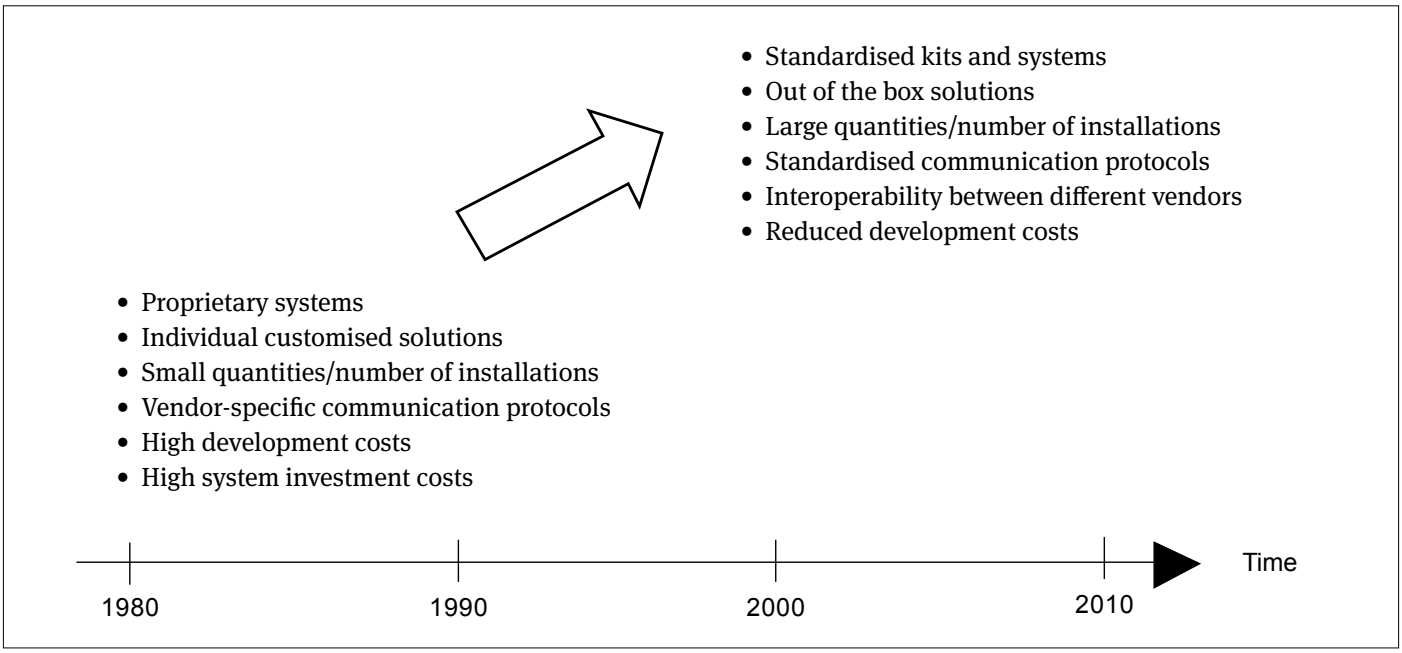

Figure 2: Development of SCADA system components.

	Internet environment	Process control environment
Reliability	Occasional failures tolerated Beta test in the field acceptable	Outages intolerable Thorough quality assurance testing expected
Risk impact	Loss of data	Loss of production, equipment, life
Performance	High throughput demanded High delay and jitter accepted	Modest throughput acceptable High delay is a serious concern
Risk management	Recover by reboot Safety is a non-issue	Fault tolerance essential Explicit hazard analysis expected
Security	Most sites insecure Little separation between intranets on same site Focus is central server security	Tight physical security Isolated office network from plant network Focus is edge control device stability

Table 1: Differences between internet and process control environments.

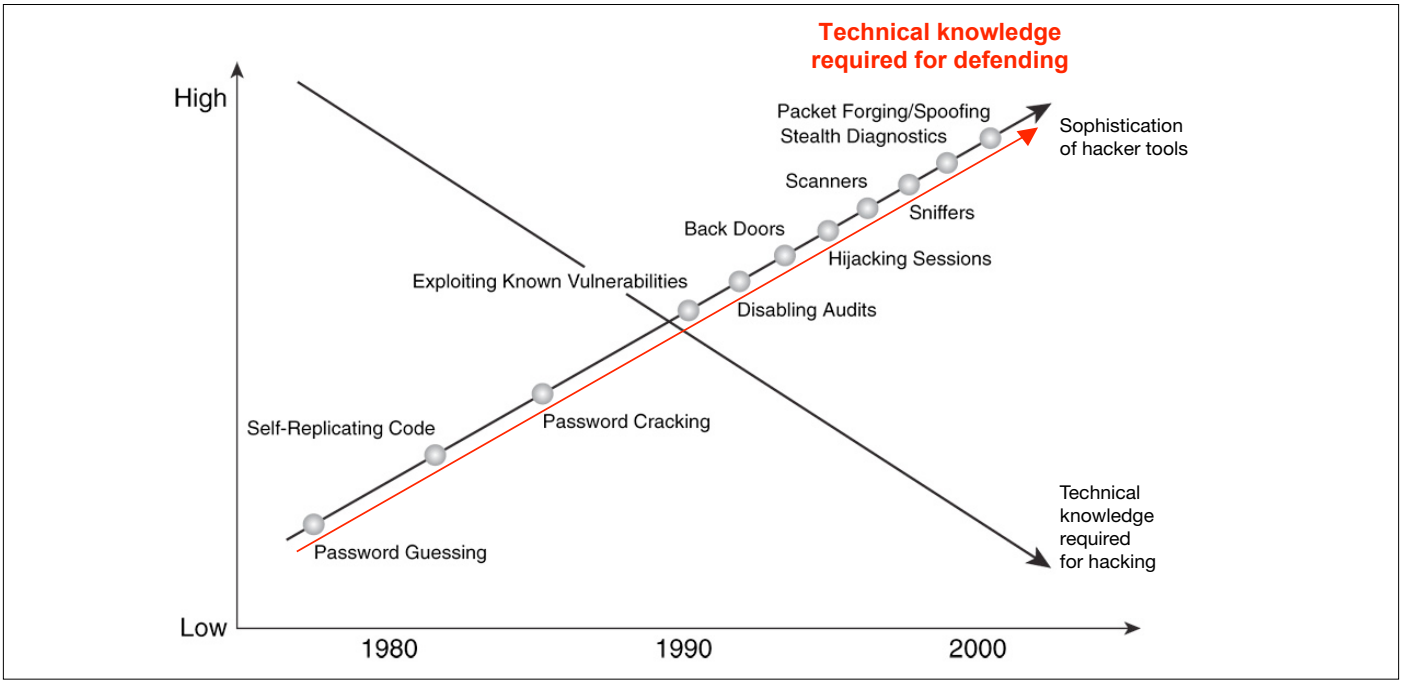

Figure 3: The sophistication of hacker tools.

The affected parties reported that for 50 per cent of these registered incidents, their losses exceeded $US1 million. The Carnegie Mellon Software Engineering Institute reports at least two cases with financial losses in the range of "tens of millions of dollars".

According to a report written by IBM's Global Security Intelligence team "the global IT threat landscape is going through a fundamental shift, or evolution, in cyber crime from pervasive global outbreaks to smaller, stealthier attacks targeted at specific organisations". This statement can be easily supported by the sophistication of hacker tools (refer to Figure 3).

The following non-exhaustive list highlights the risk potential using real examples:

- In July 2010, the computer worm Stuxnet was discovered. This was the first identified malware to subvert the PLCs of industrial control systems. The worm initially spreads indiscriminately, but includes a highly specialised malware payload that is designed to target only Siemens SCADA systems that are configured to control and monitor specific industrial processes.
- In 2004, a disgruntled former SCADA supervisor caused the release of nearly 264,000 gallons of raw sewage into the sewer system of an Australian city.
- The safety monitoring system of Ohio's Davis-Besse nuclear power plant was offline for five hours due to the Slammer Worm in January 2003.
- In 2000, the Russian government announced that hackers succeeded in gaining control of the Gazprom pipeline network.
- In 1995, at TransCanada PipeLines Ltd, disabled low pressure and temp alarms caused two pipelines to rupture and catch fire at compressor station #30.

From these examples, the following general cyber attack scenarios can be derived:

1. Issuing unauthorised commands to control equipment;
2. Sending false information to a control system operator that initiates inappropriate actions;
3. Disrupting control system operation by delaying or blocking the flow of information through the control network;

4. Making unauthorised changes to control system software to modify alarm thresholds or other configuration settings; and,
5. Rendering resources unavailable by propogating malicious software (e.g. a virus, worm, Trojan horse) through the control network.

These scenarios can be justified as realistic risk potentials as common SCADA communication protocols provide no authentication and therefore no confidentiality. Furthermore, SCADA systems are based on common hardware and operating software and are vulnerable to viruses. However, SCADA systems do rely on real-time performance, and improperly selected and configured antivirus application software could degrade a SCADA system's performance enough to make the system useless or dangerous.

These concerns are reflected by SCADA system end users, which is one of the reasons why antivirus software has not been more widely adopted within these systems. Patch management is another known problem within the IT world; changing anything in the continuous operating SCADA world is a challenging task that is often significantly delayed or never performed during the lifetime of these systems.

Specific security guidelines

A single security product or technology cannot adequately protect an industrial control system, so a multiple-layer strategy involving two (or more) different overlapping security mechanisms is desired to avoid a vulnerability in one technique from allowing a compromise.

Securing a SCADA system is based on a combination of effective security policies and a properly configured set of technical security controls. An initial list of topics, which needs to be considered within that respect are:

- A security plan with security policies needs to be in place to ensure safe and reliable operations.
- Security issues need to be addressed throughout the lifecycle of the SCADA system, starting from architecture, through to procurement and installation, and followed up during maintenance and decommissioning.
- The network topology for the process control network should be based on separate dedicated communication layers protected by firewalls. The most critical communication links should be hosted within the most secure and reliable layer.
- Security techniques, such as encryption, should be applied to SCADA communications and data storage.
- Wireless networks have an elevated level of security concern within a process control network; this needs to be carefully evaluated and assessed for risks prior to installation. Wireless network technology changes frequently, and its security depends on the ability to stay current and protected.
- Process control and corporate office networks should be logically separated through the use of a DMZ network architecture, which prevents direct traffic between these networks.
- All critical components need to be redundant and based on redundant networks.
- The process control system design needs to be fault tolerant to prevent catastrophic cascading events. System failures should shut down the plant in a secure manner.
- Physical access to the process control network and devices should be restricted. Disable unused ports and services on system devices and verify that this will not impact operations.
- SCADA system user privileges should be restricted only to those that are required to perform each person's job (i.e. establishing role-based access control and configuring each role based on the principle of least privilege).
- The use of strong authentication mechanisms for users of the process control network as well as for the corporate office network should be considered and kept separate (i.e. process control network accounts do not use corporate network user accounts). Disable any default user accounts and replace simple vendor passwords.
- Access rights given to the system vendor should be removed once the work has been completed.
- Security controls such as antivirus software and file integrity checking software should be implemented where technically feasible in order to prevent, deter, detect, and mitigate the introduction, exposure and propagation of malicious software to, within, and from the process control network.
- Security patches should be deployed after all patches under field condition have been tested on a test bed environment in a timely manner.

References

- API 1164 (2nd edition, June 2009): Pipeline SCADA Security
- API Security Guidelines for the Petroleum Industry (3rd edition, April 2005)
- Germany's Federal Office for Information Security: IT-Grundschutz
- ISO/IEC 27001:2005 (issued October 2005): Information technology -- Security techniques -- Information security management systems -- Requirements
- ISO/IEC 27002:2005 (issued July 2007): Information technology - Security techniques - Code of practice for information security management
- Journal of Computers, Vol. 5, No. 3, March 2010: "A Risk-Assessment Model for Cyber Attacks on Information Systems"
- NIST Special Publication 1058 (Version 1.0, Sept. 2006): Using Host-based Anti-virus Software on Industrial Control Systems: Integration Guidance and a Test Methodology for Assessing Performance Impacts
- VDE 2004 Congress, Berlin, October 2004 "The Myths and Facts behind Cyber Security Risks for Industrial Control Systems"
- www.wikipedia.org