TNO report

SCADA Security Good Practices for the Drinking Water Sector

TNO | Knowledge for business

samen tegen cybercrime
NICC

TNO-report

SCADA Security Good Practices for the Drinking Water Sector

TNO Defence, Security and Safety

Report: TNO-DV 2008 C096

Author: Eric Luiijf, MSc

The Hague, March 2008

Classification of Report
Unclassified

Report
This is an English translation of the report:
SCADA Good Practice voor de Nederlandse Drinkwatersector,
TNO DV 2007 C478, December 2007

Publisher
TNO Defence, Security and Safety
Oude Waalsdorperweg 63
P.O. Box 96864
2509 JG The Hague
The Netherlands
T +31 70 374 00 00
F +31 70 328 09 61

Translation
Language Unlimited B.V., Utrecht, The Netherlands

Author
Eric Luiijf, MSc

Design and layout
TNO, The Hague

Cover photo:
Oasen Drinkwater, by D. Van Eijndhoven

Printing
TNO, Reproduction The Hague

Summary

The SCADA Security Good Practices for the Dutch drinking water sector are intended to raise the standard of the entire drinking water sector's resistance to the unauthorised 'cyber' manipulation of the Supervisory Control and Data Acquisition (SCADA) and other Information and Communication Technology (ICT) systems and software in the field of PA.

Effective protection of the SCADA environment, systems and networks is necessary in order to guarantee the supply and quality of drinking water and to make sure that the systems cannot be manipulated by unauthorised third parties. The likely social effects of a breakdown in the water supply are so severe that control of the SCADA risk is essential. Possible consequences could be social unrest, effects on public health and major economic damage.

At the request of the Dutch National Cyber Crime Infrastructure (NICC) programme, which is run by the ICT Implementation Organisation (ICTU), TNO Defence, Security and Safety has described thirty-nine SCADA Security Good Practices for the drinking water sector. These have been divided into topics that are the responsibility of the business management team and topics for which the management of the technical process automation is responsible.
These Security Good Practices provide the drinking water sector with guidelines for secure SCADA use. They are based on international standards, de facto standards and successful security measures applied by other companies with SCADA.

Contents

List of tables and figures

Tables

Figures

Abbreviations

BCP	Business Continuity Planning
COTS	Commercial-Off-The-Shelf
CPNI	(UK) Centre for the Protection of National Infrastructure
DCS	Distributed Control Systems
DNP	Distributed Network Protocol
DoS	Denial-of-Service
ERP	Enterprise Resource Management
EWICS	European Workshop on Industrial Computer Systems Reliability, Safety and Security
GPRS	General Packet Radio Service
HMI	Human-Machine Interface
ICT	Information and Communication Technology
IEC	International Electro-technical Committee
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISA	Instrumentation Systems and Automation Society
ISO	International Organisation for Standardisation
LAN	Local Area Network
MAC	Media Access Control
MES	Manufacturing Execution System
MTU	Master Terminal Unit
NICC	(NL) Programma Nationale Infrastructuur Cyber Crime (National Cyber Crime Infrastructure programme)
NISCC	(UK) National Infrastructure Security Co-ordination Centre (now CPNI)
PA	Process Automation
PLC	Programmable Logic Controller
POTS	Plain Old Telephony System
RTU	Remote Terminal Unit
SCM	Supply Chain Management
TCP	Transmission Control Protocol
TNO	Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek (Netherlands Organisation for Applied Scientific Research)
UMTS	Universal Mobile Telecommunication System
VEWIN	Vereniging van Waterbedrijven in Nederland (Association of Dutch Drinking Water Companies)
VPN	Virtual Private Network
WAN	Wide Area network

1 Introduction

Process control systems and networks and, more particularly, the Supervisory Control And Data Acquisition (SCADA) systems and networks[1], form an essential link in the chain of guaranteed supply and quality of drinking water in the Netherlands.
In May-June 2007, the National Cyber Crime Infrastructure (NICC) programme used a questionnaire to make an inventory of the extent to which the Dutch drinking water sector is in control of the security of their process automation (PA) environment. An analysis study [1] showed that there are major differences in the extent of SCADA security in the various drinking water companies. The analysis study revealed that the drinking water companies run a risk with regard to guaranteed supply and quality of the drinking water, although they are sometimes unaware of it. There is, therefore, room for improvement in SCADA security. That was the reason for drawing up this report with Good Practices for the security of SCADA in the drinking water sector.

This report is structured as follows: Chapter 2 contains a brief background on what SCADA is, what growing risk factors exist and where and why the PA environment is vulnerable. Chapter 3 provides SCADA Security Good Practices for the management teams in the drinking water companies on the basis of the sector-wide analysis conducted previously [1] and international literature and standards.
The Good Practices are emphatically neither legislative measures nor requirements. For good reasons such as internal culture or of an organisational, architectural or technical nature, drinking water companies may opt for an entirely different security system that provides the same level of guarantee. Nevertheless, it is a good idea to assess any alternative system in light of the Good Practices described below, in order to ensure that all the gaps in security are closed. The Security Good Practices are closely linked to the Code of Practice for Information Security ([3], [6]), which is used by all Dutch drinking water companies as a basis for their information security in the office environment.
Formulation of the Good Practices took into account whether one or more drinking water companies already have such a particular Good Practice in place. If so, drinking water companies can ask their colleagues how they introduced the Good Practice and about their experiences working with it. This could be done through either the NICC or via a different route. Similarly, Chapter 4 comprises the Good Practices for technical PA management. Chapter 5 gives a number of references to SCADA security literature and websites where more information can be found on specific sub-topics. Chapter 6 contains the literature references and Appendix A provides two checklists itemising the Good Practices.

[1] Apart from its use in the trade literature, SCADA is used as an umbrella term for all forms of process control systems, unless a specific technology is examined.

2 SCADA and SCADA security

This chapter comprises a brief explanation of what SCADA is, what the growing threats to them are and where and why the PA environment is vulnerable. With the consent of the Dutch Ministry of Economic Affairs, the content of this chapter is based on the TNO-KEMA report entitled '*SCADA (in)security: a role for the government?*' [2], in which the SCADA information security problem is dealt with in detail, including an overview of national and international initiatives and other activities in the area of SCADA security.

2.1 What do the terms SCADA, PCS, DCS, RTU and PLC mean?

For PA, the ISA-95 model [14] for production modelling distinguishes five hierarchical levels in production (see Figure 1). These are:

- level 0: The physical level: sensors, actuators and process equipment;
- level 1: Sensor output, commands for actuators and computerised control and monitoring (PLC);
- level 2: Supervisory control level (SCADA) and Human-Machine Interface (HMI);
- level 3: Manufacturing Execution System (MES): support of the best possible use of production resources, base materials and people (in short: resources) for production (operations);
- level 4: Enterprise Resource Planning including business planning and logistics such as Enterprise Resource Management (ERM) and Supply Chain Management (SCM).

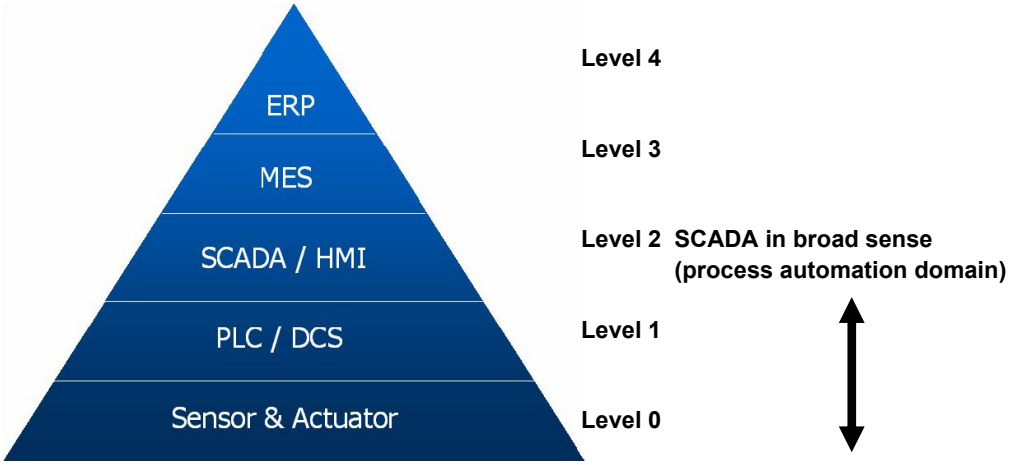

Figure 1 ISA95-1 model for production modelling.

SCADA/HMI, Level 2 in the model, performs the following tasks:

1 Visualisation and operation of process components in various places (human-machine interaction).
2 Controlled data exchange with the process control level, usually *Programmable Logic Controllers* (PLC).
3 Alarm management, trend analysis and reports.
4 Logging and storage of historical data ('historian').
5 Handling batch operations – optional in a SCADA package.
6 User management.
7 Data analysis and processing.
8 Controlled data exchange with the MES level/the administrative domain.

It is important to be aware of the fact that each of these levels has its own security measures. However, this report looks at the information security of the bottom three levels and the exchange of information with the higher levels.

The main system components on the ISA95-1 levels zero, one and two and their functions are then discussed in brief. A complete overview of the various SCADA - system components and their functions can be found in Table 1. Local processors collect measurement data from sensors and control valves, motors, etc. using hydraulics, pneumatics and power electronics. These kinds of local processors are called Programmable Logic Controllers (PLC) when they consist of a processor on one electronics board. Often, several PLC are built into a single rack or housing. A *Remote Terminal Unit* (RTU) is a local processor, usually with more processor capacity than a PLC, which operates a series of electronics board. The various systems usually communicate by means of open communication protocols, such as TCP/IP.

Example
'Intelligence' on level 1 detects a leaking pipeline using liquid sensors or a difference in flow speed or pressure (level 0). This can then be sent to a (central) control centre (level 2) as a message. An alarm is generated in the centre or the maintenance team is notified automatically. The alarm can also be displayed on an operator's screen in a logical and organised manner.

SCADA is a specific implementation of process control systems (PCS). Another PCS architecture based on distributed control is called Distributed Control Systems (DCS), which monitors and controls systems from the measuring instrument to the control console. Normally speaking, process control systems are spread over large distances and sometimes have pre-programmed control functions in the central computer system. DCS are used in large stand-alone facilities where the local processor provides the control functions. The difference between SCADA and DCS is becoming less and less clear-cut, which is one of the reasons why most of the literature (including this report) uses the term SCADA generically. In the broadest sense, the term SCADA can be seen as the domain of PA.

Table 1 Terminology and functions.

Component	Functions
Sensors and instruments	Sensors and instruments in the field that detect conditions such as voltage, power, pressure, temperature, flow speed and valve status.
Actuators	Actuators such as pumps, valves, motors and circuit breakers that are operated remotely or locally.
Local processors	Local processors communicate with both the sensors and actuators and the functions in the network. They can play one or all of the following roles: • Collection of data generated by the sensors and instruments. • Activation and deactivation of the connected actuators by means of internal (programmed) logic or based on commands sent by the operating personnel or computers. • Translation of communication protocols so that several process control systems and instruments can communicate with one another. • Identification of alarm conditions. At the moment, local processors have a number of different names, such as Programmable Logic Controller (PLC), Remote Terminal Unit (RTU), Intelligent Electronic Device (IED) and Process Automation Controller (PAC). A single local processor can be responsible for the collection of data and the control of dozens of instruments and actuators.
Short-distance communication equipment	Short-distance communication equipment ensures the communication between the local processors and the sensors and actuators. The analogue or digital signals are transmitted along relatively short cables or wireless connections.
Central Computer System	The Central Computer System acts as the central control and operating system, allowing the operating personnel to monitor the processes, receive and assess alarms, analyse data and send control signals to actuators. In some cases, the system includes programmed logic used to control the local processors automatically. In other cases, this system is purely an interface between the operating personnel and the local processors. Other tasks performed by the central computer system involve the storage of measurement data and system conditions in a (historical) database and the generation of reports. The central computer system can also be called the Master Terminal Unit (MTU) or the SCADA server. In a number of cases, it is simply a personal computer (PC) with Human-Machine Interface software (HMI).
Long-distance communication equipment	Long-distance communication equipment is responsible for the communication between the local processors and the central computer system. The network stretches for several kilometres. It uses leased lines, xDSL, dark fibre, satellite links, microwave links, point-to-point connections, GSM, GPRS, UMTS and frame relay.

2.2 SCADA use in the drinking water sector

In a broadest sense, SCADA systems and networks - or PA - form an essential link in the chain of guaranteed supply and quality of drinking water in the Netherlands. The SCADA systems in the drinking water sector measure, control and monitor (integral alarm and event handling) the following drinking water processes, both locally and at distance:

- water extraction and/or the collection of raw water;
- transport of raw water to collection basins and settling basins;
- transport to the water purification/filtration processes;
- monitoring and control of water purification and filtration processes;
- monitoring and control of the quality control process;
- treated water distribution, and
- control of pressure-boost pumps.

This includes the monitoring and control of the flow speed in pipelines, the pressure in storage tanks, switching pumps on and off, controlling valves and monitoring aspects of water quality such as the pH value and cloudiness. The alarm display and intervention options are mostly concentrated in a control and monitoring centre. In the drinking water sector, this is often known as the ‘central watch’.

2.3 SCADA insecurity and the risk

The fact that SCADA systems and networks are increasingly insecure is the result of a number of technical and organisational developments. Firstly, SCADA is a product of classic PA with racks full of electronics and relays, an environment in which information security played no role whatsoever. Neither was it necessary, since the SCADA systems and protocols were based on:

- proprietary protocols, techniques and underlying control system;
- no public information on how SCADA worked;
- no telecommunications or only point-to-point connections via leased or owned lines;
- no connections to the administrative business network and the Internet;
- implementations without adequate security mechanisms because the environment was assumed to be hacker-free;
- protocol implementations that took no account of ‘stress conditions’ like those that can be caused by network overloads or improper protocol behaviour;
- systems that did not have to be patched;
- totally controlled and closed secure environments.

Nowadays, the practical situation is different. The basic principles mentioned above no longer apply. Unfortunately, it is often the case that in terms of information security, neither the applied SCADA technology nor the operational environment has evolved along with the rapid operational and technical developments:

- SCADA protocols have become open standard; their description can be found on the Internet.

- SCADA runs as an application on Windows or Linux and uses Internet protocols (TCP/IP) for the transfer of data. The vulnerabilities of those systems and protocols are known by hackers all over the world and can be exploited using toolkits.
- The current human-machine interface no longer requires complicated commands, and is based on a web browser interface.
- For the business world, it is necessary to create links to company networks and public networks. There are also modem access points to the SCADA network for control from home and for maintenance by manufacturers and SCADA suppliers.
- Hackers and others are becoming increasingly interested in breaking into SCADA systems and networks.
- Simple tests show that SCADA systems become stressed or even break down altogether as soon as an unknown package is sent to them via the network.
- A new option on PLC boards that cannot always be disabled is an integrated web server which gives remote access to all parameter settings.
- SCADA equipment sometimes includes a standard modem to enable remote access by the SCADA supplier.
- Passwords are never changed and are not personal, because 'the environment is closed, isn't it?'

This all takes place in a PA environment that is largely unaware of the SCADA risk (see also the various examples in [9]). This environment usually supports a totally different culture than the one in the world of corporate automation, where information security receives more attention and where protection against hackers, viruses, Trojan code and spam is the order of the day [10]. In addition, organisations that apply PA have not progressed along with the developments in protecting PA. Security is not embedded in the operating process and it is often unclear who the process owner is.
Previous analysis [1] has shown that a number of aspects in the SCADA process automation environment of the drinking water companies are no different:

- there is often no SCADA-specific security policy;
- hardly anything is done to make personnel more security aware;
- no risk-limiting measures are taken for recognised risk factors ('what keeps the sector awake at night'?);
- third parties can connect equipment to the SCADA network without supervision;
- virus and worm scans are seldom performed;
- the necessary patches are not installed or installed late.

Table 2 More misconceptions about the invulnerability of SCADA.

Assumption	Reality
We use leased lines, so nobody can access our communication connections	It is easy to tap into these communication lines (see www.tscm.com/outsideplant.html, for example).
We use dial-up connections and nobody knows the telephone numbers	A tap on the outgoing line or an itemised telephone bill quickly reveals all numbers that have been called. War dialler software automatically calls a series of numbers and can identify the numbers that have a modem connection.
We use call-back modems so unauthorised parties cannot gain access.	If a connection can be tapped, it is easy to get around the call-back mechanism. There are even methods for which a tap is unnecessary.
Our remote systems are protected by passwords.	The methods used to steal passwords are common knowledge. The easiest method is to eavesdrop on the data traffic with a sniffer. The password can then be intercepted when it is sent as normal text over the communication line. Password guessing methods with the aid of a dictionary are also well known. The exchange of passwords or never changing a password is also extremely common. All too often, a password is too simple with only a few characters and this is never changed.
We use frequency modulation technology like that used by the military for secure communication.	There are simple methods for decoding frequency modulation series. The Wireless LAN Association recommends the use of encryption on all networks, even on frequency modulation networks.
We use a protocol that is only known to the supplier and a few other people; intruders cannot understand our SCADA messages.	Even the protocols owned by certain suppliers are more generally known that most people realise. Suppliers, consultants and current and former employees of a company and other companies that use the same SCADA protocol know all the details. Manuals and software for analysing the protocols can be found on the Internet.

2.4 Incidents involving SCADA in the drinking water sector and other sectors

The threats to PA can be broken down into:

- Organisational threats such as a lack of security policy, a lack of attention to security awareness, poorly regulated access to the systems, no password policy, etc.
- Physical threats such as explosions, fire or vandalism.
- Technical threats such as software and hardware malfunctions, viruses, denial-of-service attacks, etc.

All over the world, incidents involving SCADA are hardly ever publicised, and when they are, this often takes place outside Europe. European companies prefer to keep incidents quiet or only report a ‘technical malfunction’. The Dutch SCADA report [2] contains a list of publicised incidents involving SCADA systems in a number of sectors. Drinking water companies have only made a few incidents public on the

international stage. At least one SCADA security incident has occurred in the Netherlands.
The following are some examples of publicised incidents in the drinking water sector:

- **Manipulation of drinking water and sewage treatment plants, Australia**
  The most commonly cited example used to demonstrate the vulnerability of SCADA systems and networks is that of former contractor Vitek Boden's unauthorised access to the process control system of the drinking water and sewage treatment plants run by Hunter Watertech in Maroochy Shire, Australia. Boden was the site engineer who installed SCADA systems for Hunter Watertech. The SCADA system comprised a local processor at each of the over 300 pumping stations. Each local processor communicated with the central computer system via a radio link. Boden resigned from his company as the project was nearing completion in 1999 having worked on it for two years, and asked Hunter Watertech for a job. They refused to employ him and shortly thereafter, the pumping stations for the sewage system began to malfunction and valves in the drinking water system started closing on their own volition. During a police check on 23 April 2000, the police discovered a PC and radio transmission equipment in Vitek Boden's car. He subsequently admitted to 46 cases of remote manipulation of the Hunter Watertech SCADA systems. He deactivated alarms, interfered with communications, stopped pumps from starting up at the right time and was responsible for the overflow and release of untreated wastewater. It is estimated that between January 2000 and 23 April 2000, almost a million litres of untreated sewage water was released into the environment.[2]
- **Destruction of a SCADA system in Tshwane, South Africa**
  On 18 August 2006, vandals destroyed the SCADA system at a reservoir in Tshwane, South Africa. The result was that Mamelodi and Eersterust (Pretoria) had no drinking water for eleven days.
- **Hacker in drinking water filtration system, Harrisburg, Pennsylvania, USA**
  A hacker got into the SCADA of the drinking water filtration system in Harrisburg, Pennsylvania, USA. He did so by remotely hijacking the laptop of one of the drinking water company's employees after installing Trojan code. As soon as the employee logged in from home, the hacker was able to penetrate the SCADA network via the laptop using the Internet. The hacker then installed malware (Trojan software) and spyware on the SCADA systems. In theory, the intruder was then in a position to take over the SCADA network, give false commands and totally overload the network.[3]
- **Communication problems in the drinking water distribution system, Fort Worth, USA**
  On 14 January 2007, communication problems with the decentralised SCADA systems caused an eight-hour breakdown in part of the drinking water supply in Forth Worth. All control of the pumps and stock tanks was lost.

[2] http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/
[3] http://blogs.abcnews.com/theblotter/2006/10/hackers_penetra.html

- **Hacker penetration in a drinking water system, USA**
  The American Water ISAC reported that in 2000, a SCADA system at a drinking water company was penetrated by hackers.
- **A software error in SCADA** was responsible for an excessively low chlorine level, rendering the drinking water undrinkable in Lewiston, MA, USA (2003).

Published incidents involving SCADA systems in other sectors are examples of insecure aspects of SCADA referred to previously in paragraph 2.3:

- Weak and often unsecured SCADA protocols leading to system failure.
- Weak or unsecured communication links between company networks and the outside world allowing hackers and viruses to get in.
- Maintenance suppliers who can get around set security measures due to a lack of oversight of what equipment may be connected (even in a nuclear power station).
- Lack of change management.
- Lack of physical protection and security of SCADA systems and networks.

> 24/08/2007 http://www.zone-h.org/content/view/14811/30/
> Doing penetration tests can bring sometimes surprising results. But doing penetration tests on critical targets should not bring any surprising results.
> Scott Lunsford was offered to penetrate into a nuclear power station.
> As owner of the plant claimed, critical components could not be accessed from the Internet. 'It turned out to be one of the easiest penetration tests I had ever done', Lunsford said. He added: 'By the first day, we had penetrated the network. Within a week, we were controlling (the SCADA of) a nuclear power plant.'

2.5 Need for SCADA security in the drinking water sector

Effective security of the SCADA environment, systems and networks (levels 0, 1 and 2 in Figure 1) in the drinking water sector is necessary to guarantee the supply and the quality of drinking water and to ensure that the SCADA systems cannot be manipulated by unauthorised parties. The hacker problems, viruses and loss of communication between SCADA network components referred to above can also occur in the Dutch drinking water sector and elsewhere.
The likely social effects of a breakdown in the water supply are severe.
Possible consequences could be social unrest, effects on public health and major economic damage. Therefore, the critical drinking water infrastructure companies must be in control of their SCADA risk as part of the total company risk.

To summarise, it can be concluded that effective security of SCADA systems and networks in the drinking water sector is essential. This security requires an approach in which equal attention is paid to the organisational, physical and technical aspects of information security. The following Good Practices for SCADA security in the drinking water sector provide guidelines for the management team and technical process automation management.

3 Good Practices for the management team

To find effective solutions to mitigate the SCADA risk aspects discussed in the previous chapter, this document contains a number of SCADA Security Good Practices. Good Practices are emphatically neither legislative measures nor requirements.
For good reasons such as internal culture or of an organisational, architectural or technical nature, drinking water companies may opt for an entirely different security system that provides the same level of guarantee. Nevertheless, it is a good idea to assess any alternative set of security measures in light of the Good Practices described below, in order to ensure that all the gaps in security are closed.

The Good Practices are divided into two groups. The first group comprises the Good Practices at company management level. They are contained in this chapter. The next chapter lists the Good Practices at the technical process automation level.

The Good Practices for the drinking water sector at company management level are an extension of the general information security policy that already exists in the drinking water sector and are geared towards the general corporate culture of risk management. The Good Practices have been clustered under the following main topics:

- Company security policy and specific SCADA security policy.
- Risk management.
- Audit.
- Acquisition policy for SCADA systems, networks and services.

3.1 Company security policy and specific SCADA security policy

The right implementation of information security for SCADA systems and networks requires an environment in which management pays attention to security. This involves security policy embedded in the operating process on the basis of related risk analysis and a risk management process that applies to the entire drinking water company.

Good Practice 1
The drinking water company has a general information security policy and a specific SCADA security policy that is inextricably bound up with that general information security policy.

Good Practice 2
The general information security policy is based on the Code of Practice for Information Security [3] and the associated security management system [6].[4]

[4] Note: the security monitor of the VEWIN and the Amsterdam Municipal Information Security Standard (GIBN) are derived from the Code of Practice for Information Security.

Good Practice 3
The basic premise for the specific SCADA security policy is that it can be implemented in such a way that for the employees, measures taken form a logical extension of the general (information) security policy and the security of the office environment (OA).

Good Practice 4
The specific SCADA security policy should include the physical protection of the SCADA systems and networks.

Good Practice 5
For the SCADA environment, the security responsibilities, duties and authorities are laid down for management staff and SCADA users (see also [8] point 12).

Background
- The lack of SCADA-specific security policy, security procedures and security culture top the American Top 10 of SCADA vulnerabilities [10].
- Lack of an information security policy and lack of a risk analysis leads to the ad hoc implementation of security measures, so it is never clear whether the right security measures have been taken and what gaps in security exist.
- The information security policy based on the Code of Practice for Information Security includes a number of controls that are not directly suitable for the 24-hour-a-day/ 7-days-a-week SCADA environment. According to [4] and [5], a number of the control elements that are included in the Code of Practice require some degree of supplementation. The main elements are: outsourcing, co-ordination of information and process security, physical security of the ICT environment (i.e. the SCADA environment), operational procedures in a 24/7 operational environment, antivirus policy, logging and alarms, access controls, password policy (see also section 4.6) and business continuity management. This is why it is advisable to develop a separate, supplemental security policy for SCADA. It is also wise to have a clear-cut line for reporting any security incidents that may occur (see also the Code of Practice for Information Security [3], section 11.2).
- Elements contained in the current, regularly updated SCADA security policy document are security goals, security organisation, rules and procedures that are clearly and intelligibly derived from the drinking water company's business objectives (guaranteed supply and quality of drinking water). What are the roles and responsibilities of the specific positions and of other employees who are involved in or work with PA? What is explicitly forbidden and what is expected of the employee or management staff member when a (potential) security incident is detected by them?

3.2 Risk management

Good Practice 6
The process automation/SCADA environment forms an integral part of the risk management process at the highest company level.

Background: The process automation/SCADA environment is an essential part of the drinking water operating process that guarantees the supply and quality of the drinking water. The security in all its aspects (availability, reliability, integrity, confidentiality) of the SCADA systems and networks, the risk analysis, risk management and the related business continuity planning (BCP) are all geared to it.

3.3 Security awareness

One of the main risk factors that requires internal control is the human element. This forms a major risk factor in the SCADA environment as well. Security awareness helps the management (exemplary function) and the employees to remain focussed in terms of their attitudes towards security as well as helping to improve the organisation's security level.

Good Practice 7
The drinking water company has a continuous security awareness programme.

Background: Effective information security requires constant attention to security awareness and the employees' attitude towards security, particularly when it concerns critical operating processes. If the drinking water company employees are not security aware, this will be felt by third parties (suppliers, maintenance and repair technicians) who have to work on the SCADA systems and networks, aggravating the potential risk of deliberate or unconsciously influencing the SCADA systems and hence the drinking water process in an unauthorised way
(see also [8] point 21).

3.4 Audit

Good Practice 8
An EDP audit of the SCADA systems and networks is conducted at least once a year.

Background: Section 393 in Part 2 of the Dutch Civil Code states the following concerning the annual accounts: '*The accountant submits a report on his audit to the Supervisory Board and the Board of Management. This will minimally include a record of his findings with regard to the reliability and continuity of the automated data processing.*' This section of the law is part of the Computer Criminality Act I. The reason for assigning this extra task to an accountant is as follows: in the case of computer hacking, cyber terrorism or any other form of computer criminality, an arrested and prosecuted perpetrator appearing in court can put forward a defence that he or she did not know that he or she was breaking in, that there was no form of security whatsoever and that he or she accessed a system or network without any

trouble, etc. The lawyer of the perpetrator(s) may demand that the drinking water company proves that a sufficient level of security is in place. In short: 'submit all your security plans and details' to the court and hence make them public.
This is reason enough for most companies to refrain from prosecution and not make their security measures public, usually allowing the perpetrator(s) to get off scot-free.

According to the Civil Code, the auditor's report issued as part of the annual accounts - if present and *in this case, demonstrably covering the SCADA systems and networks* - is sufficient to demonstrate that you met the statutory requirements of '*some degree of security'* that the suspect knowingly penetrated. It is then not necessary to submit detailed information on the security measures taken. The risk of not having an auditor's report issued as part of the annual accounts that explicitly include the SCADA networks is, therefore, that prosecution of the perpetrator(s) is considerably more difficult, together with the risk of sensitive security measures being made public.

The audit will, at the very least, examine the following:
- Password and access policy.
- The security of the connections between the SCADA systems and networks, on the one hand, and office automation, public networks and the Internet, on the other (see also [8] points 9 and 18).
- The security status of remotely monitored and controlled locations (see also [8] point 10).
- Possible modem access points.
- The method of reporting security incidents, security logging and the follow-up.
- The physical and electronic protection of the SCADA system components and networks (see also [8] points 10 and 18), such as locks on housings, alarms on doors and so on.

In addition to a formal audit, it is also advisable to conduct an internal security audit several times a year that can be synchronised with phases in the security awareness programme.

3.5 Acquisition policy for SCADA systems and services

Information security applies to the entire life cycle of SCADA equipment, software and services. Acquisition is an important step where the internal security requirements can be imposed on suppliers and third parties. It also helps to make clear to external parties that the drinking water company tackles security in a professional, serious manner.

Good Practice 9
The contracts to be signed with suppliers for (large) SCADA systems and networks include a continuity clause intended to guarantee the supply and quality of drinking water:

1 The supplier undertakes to keep enough spare parts in stock for an agreed number of years.
2 The supplier guarantees that in the case of a disaster, they will provide support in seeking a solution.
3 In the event that the SCADA system and/or network is lost for any reason whatsoever, the supplier will provide priority co-operation in the replacement of the SCADA system and/or network.
4 The supplier verifies patches from third parties that supply essential system components (the Microsoft operating system, for example) within a short lead time and makes these available in a trusted and reliable manner.

Background: To guarantee the supply and quality of drinking water, the SCADA systems that monitor and control the critical drinking water processes should be functional again as soon as possible after an ordinary malfunction or a disaster occurs.

Good Practice 10
Prior to acquisition, the drinking water company sets requirements for information security which the SCADA systems, networks and software are expected to meet. See also Chapter 12 of the Code of Practice for Information Security [3].

Background: Since a SCADA system and network are often introduced as an integral project, it is important to decide in advance what security requirements the system to be delivered has to meet. [7] contains a series of initial suggestions for technical requirements. Also stipulate that, without explicit permission, suppliers are not permitted to inform third parties that they have supplied SCADA systems to your drinking water company.

Good Practice 11
The maintenance and support contracts signed with third parties include a security clause.

This will, at the very least, regulate the following:

1 Compliance by maintenance and support technicians with the prevailing company security policy for SCADA systems and networks.
2 Clearance and access agreements for maintenance technicians.
3 Guarantees regarding the protection of confidential company information (see also [8] point 21).
4 Supervision by the drinking water company of the work to be performed by the third party.
5 Disposal of (defective) information carriers bearing possible sensitive company information.

Background: The prevailing company security policy for the SCADA systems and networks also applies to third party employees. The prime stipulation is restricted access to the SCADA systems. Third parties must minimally provide guarantees that their employees are trustworthy (e.g. by means of third party liability for all of their employees' actions, a Certificate of Good Conduct, etc.). The conditions under which third party equipment and software (including laptops for the maintenance technician, modem) may be connected to the SCADA systems or network have been agreed and laid down in writing. All work performed by third parties on the systems and network components in the SCADA environment is supervised. This prevents serious breakdowns that jeopardise the guaranteed supply of drinking water (see also [8] point 7). Deviations from the procedure are only allowed with the permission of the security manager of the drinking water company.

Defective information media that are embedded in SCADA systems that have to be replaced (hard disks and ROM modules, for example) may bear sensitive company data. It has to be agreed that any such information will not leave the premises of the drinking water company until it is ensured that the sensitive information has been properly erased or destroyed.

4 Good Practices for the technical PA management

The Good Practices are clustered under the following main topics:
- Defence in depth.
- Separated SCADA and office automation environments.
- Secure links to the SCADA environment.
- Secured SCADA systems and network components.
- Secure protection of the SCADA environment.
- Password policy for the SCADA environment.
- Business continuity and the SCADA systems and network components.
- Management of information media in the SCADA environment.

These Good Practices were drawn up on the basis of information from a number of sources, including drafts of standards still under development: [3], [11], [12], and [13].

4.1 Defence in depth

Good Practice 12
The SCADA environment is secured according to the principle of defence in depth.[5]

Background: The accessibility of the SCADA systems and networks from public networks and from the company network is screened off and secured to such an extent that breaking through one security measure does not allow uncontrolled access to the SCADA systems and network. In addition to firewalls, easy-to-check network links, and call-back systems, security measures such as authentication on the basis of individual, regularly changed passwords, intrusion detection (see also [10] point 7), antivirus measures and patch policy can be used to erect barriers to repel hostile attacks. This increases the risk of discovery of an attacker and reduces the risk of intrusion. See also [10], point 2.

4.2 Separated SCADA and office automation environments

Good Practice 13
The SCADA environment is secure and strictly separated from the office automation environment (OA).

Good Practice 14
With a logical partition between the office automation (OA) environment and the SCADA/PA environment with a shared network infrastructure, the control of the SCADA environment will definitely not be lost in the event of an OA network overload.

Background: A strict and, in particular, simple partition between the OA environment and the SCADA/PA environment significantly increases the security

[5] See also [10], vulnerability number 2.

and reliability of the SCADA environment. SCADA systems and SCADA software are highly sensitive to unexpected packages distributed by worms and to network overloads. This risk should, therefore, be contained.
If VPNs and concentrators are employed by the KA and the SCADA/PA environment for the simultaneous use of the same network and transmission components, there is a risk of Trojan code or a worm causing an overload on the (logical) OA network.
In such cases, not all concentrators and VPN networks provide sufficient capacity to the SCADA network, resulting in a loss of monitoring and control of SCADA systems.
It is, therefore, a good practice to test the sensitivity of the SCADA network for overloading on the OA side. This should be done under controlled conditions at least after every network configuration change that potentially may affect the availability of the SCADA environment.

4.3 Secure links to the SCADA environment

Good Practice 15
Remove any non-essential links between the SCADA network and other networks.

Good Practice 16
On the basis of the prevailing security policy, perform a thorough, continuously monitored control of the remaining link(s) and the information that passes across those link(s). (See also [8] points 1, 2 and 3).

Good Practice 17
If a link between the SCADA environment and an OA network is necessary, it is protected by a firewall that only admits the required and approved services.
The logging of the firewall is checked on a regular basis and analysed for unauthorised traffic or attempts to that end.

Good Practice 18
The SCADA environment is never linked directly to the Internet.

Good Practice 19
The SCADA environment does not use the Internet to transfer information, unless a separate risk analysis has been conducted regarding denial-of-service (DoS) attacks and loss of the Internet infrastructure.

Good Practice 20
SCADA networks have no wireless access points (WiFi), unless a separate, regular expert risk analysis shows that the risk is under control. Use all available security options (no visible aerials, no beacon packets, highest form of encryption, such as WPA2, MAC control, for example). See also [10], point 5.

Good Practice 21
Modems or other external access points should be monitored constantly and fitted with a reliable and strong authentication mechanism. Authorisations for remote access should be examined regularly to see if they need to be continued. The basic

premise is that authorisations are only issued if they are strictly necessary (see also [8] point 7 and [10] point 3).

Good Practice 22
The security measures and settings of the network separators (firewalls, routers, VPNs) and links (modems) are verified on a regular basis.

Background: Where possible, unauthorised manipulation of the SCADA environment is rendered impossible. Links from the SCADA environment to other environments are weak spots. It is, therefore, essential for the drinking water companies to monitor these links on a regular basis. For internal links, a properly configured and maintained firewall can serve as an extra layer of defence in depth. Direct links to the Internet are vulnerable to break-ins, attacks on the availability of SCADA systems and networks and loss of access (e.g. power failure, cable problems). If the Internet and other public networks are used for teleworking services, it is advisable to use a sophisticated form of authentication. It is also wise to have a plan ready in the event of malfunctions in the communication infrastructure and the power supply.

4.4 Secure SCADA systems and network components

Good Practice 23
The SCADA systems are 'hardened' and the SCADA security measures provided by the manufacturer are utilised to the fullest extent.

Good Practice 24
The configuration process of the SCADA systems and network components has been documented.

Good Practice 25
The configuration modification of the SCADA systems and network components is a controlled process.

Good Practice 26
Wherever possible, SCADA systems are protected by the latest antivirus software.

Background: Hardening of the SCADA system means that the system is configured in such a way that:

1 Known vulnerabilities have been removed.
2 All processes that are not essential for the correct operation of the system have been removed from the configuration.
3 All unnecessary ports and services have been deactivated and blocked.
4 All default access points have been removed.
5 It makes optimum use of the security options provided by the manufacturer within the bounds of the drinking water company's SCADA security policy framework.

Hardening and the use of available security options are intended to reduce the number of vulnerabilities that may give access to hackers and malware (see also [8] points 4 and 6). Well-documented internal systems and their configurations matched with a configuration modification process increase the chance of a faster recovery in the event of serious breakdowns or the loss of SCADA systems and networks.

SCADA systems, including those in the drinking water sector, are increasingly based on commercial off-the-shelf code (Windows, Linux, Open SCADA, etc.). They are also linked to networks with a multi-stage Internet connection or subject to third-party equipment that is connected to the SCADA network.
Early detection of hostile code (malware) such as viruses, worms and Trojan code in the SCADA environment can help to keep the SCADA systems and network free of malware. Antivirus software is kept up to date to prevent malware affecting the SCADA environment and thus the guaranteed supply and quality of the drinking water.

Good Practice 27
Formulate a patch policy for the SCADA systems and network components that is in line with the acceptable risk of security breaches by hackers, and by viruses, Trojan code and other forms of malware.

Background: The existence of vulnerabilities in software and systems becomes quickly known to the hackers. Once they are, it takes cyber criminals no more than a few days to build 'exploits' to take advantage of these vulnerabilities. As soon as a patch is issued by a supplier, hackers use reverse engineering to break open unpatched systems. SCADA suppliers are often slow to verify patches from Microsoft and other software vendors, so SCADA systems run a higher risk until the patch is verified and then implemented by the drinking water company.
It is essential to install patches quickly to keep the risk of infection to a minimum, particularly when third parties can connect their own systems (e.g., laptops) to the SCADA network.

4.5 Secure protection of the SCADA environment

Good Practice 28
Only authorised staff are allowed physical and electronic access to the SCADA systems and networks.

Good Practice 29
Only pre-authorised equipment may be connected to the SCADA network.

Good Practice 30
As a rule of thumb, third parties never connect equipment (e.g., laptops) to the SCADA network and other company networks. If an exception is made for operational reasons, the equipment/software in question should be scanned for worms and viruses with the latest virus signatures *before* being connected.
The connection itself should be carried out under the supervision and responsibility of an employee of the drinking water company.

Background: A third party can unwittingly install a virus, worm or Trojan horse or perform unauthorised activities. Laptops and other equipment belonging to third parties are not always subjected to strict security checks. This kind of equipment can provide third parties with unwanted access to the SCADA environment if it (accidentally) also supports a wireless network connection. This kind of unsupervised access is often granted while the management claims to be having sleepless nights worrying about unauthorised activities being carried out by third parties and the risk of viruses being brought in by third parties to the process control environment.

4.6 Password policy for the SCADA environment

Good Practice 31
The default user name – password combinations set by the manufacturer are immediately replaced by combinations chosen by the drinking water company.

Good Practice 32
Passwords that allow access to essential system functions are complex, are only given to company employees on a need-to-know basis, and are changed regularly.

Good Practice 33
Personal passwords are not known to others and are changed regularly.

Background: To gain access to services in the SCADA network, users are first required to authenticate themselves. Depending on the desired complexity, this can be done in one step on the basis of knowledge (user name - password combination), or in multiple steps by the additional use of something a user demonstrably has (a token) or is (a biometric feature). Security based on passwords only is regarded as the weakest form. The weakness of a password partly depends on the way in which a user treats it. The risk of a password being discovered by an unauthorised party depends on minimal password requirements (length, type of characters, not from the dictionary, etc.), the frequency of use and how often the password is changed.
Section 11.2 of the Code of Practice for Information Security [3] contains a number of management controls regarding passwords and password policy. Since SCADA systems are used 24/7 and often comprise distributed components, special attention is required for password use and the related requirements:

- The first principle in information security is that when a new system is used for the first time, default passwords are removed or changed. Apart from the fact that standard manufacturer passwords are usually easy to guess, they are also publicly documented. The system and hence the network is then wide open. See also [10] point 3.
- Principle number two is that every user has a personal, secret password that is not to be shared with anyone else. The Code of Practice for Information Security is extremely strict on this point, because then each user can be held individually responsible for his or her actions. Group identification is only permitted when it is ‘suitable for the work to be performed’.
- Depending on the size of the organisation, staff turnover and the presence of third parties, it is a good idea to change passwords regularly. In the case of group-

related passwords, it is advisable to change the password as soon as a member of the group leaves the company.

4.7 Business continuity and the SCADA systems and network components

Good Practice 34
The business continuity management system of the SCADA systems and network components is designed in accordance with Chapter 14 of the Code of Practice for Information Security [3]. An important aspect of this system is that the drinking water company has a well-maintained and regularly practised continuity plan in place for the essential elements in the SCADA environment.

Good Practice 35
The essential data in SCADA systems and network components is regularly backed up (see also [8] point 19).

Good Practice 36
SCADA back-up media is stored securely at a remote location.

Good Practice 37
Part of the quality process comprises regular verification to ensure that the back-up information can be used during a system recovery operation (see also [8] point 19).

Good Practice 38
The drinking water company has a well-maintained and regularly practised continuity plan for the essential elements in the SCADA environment (systems and network components).

Background: Disasters in the SCADA environment may occur. They may include hardware and software malfunctions, the consequences of a lightning strike, fire, water damage, power problems, etc. Rapid deployment of redundant systems, reconfiguration and efficient recovery/reload of the SCADA systems in a controlled manner requires advance planning and practice to guarantee the supply and quality of the drinking water.

4.8 Management of information media in the SCADA environment

Good Practice 39
Information media used in the SCADA environment are managed both effectively and in a controlled manner during their full life-cycle including the disposal process.

Background: Information media used in the SCADA environment may bear sensitive company information such as configuration data. When equipment containing built-in information media such as hard disks is replaced by new equipment or information media themselves are replaced, it is advisable to erase the data thoroughly or to destroy the information media.

5 Background literature

5.1 Management of Information Security

- H.A.M. Luiijf, MSc and R. Lassche MSc, *SCADA (on)veiligheid: een rol voor de overheid?(SCADA (in)security: a role for the government?),* TNO-KEMA report, April 2006.
- ISO, Information technology – Security techniques - *Code of practice for information security management framework*, ISO/IEC 17799:2005.

  Subsequent versions of the Code will be published under number ISO/IEC 27002.
  The international version is available via www.iso.ch; local language versions exist.
- ISO, Information technology -- Security techniques -- *Information security management systems -- Requirements,* ISO/IEC 27001:2005.

  The certifiable management framework that forms part of ISO/IEC 17799:2005.
- G. Finco, et al., *Cyber Procurement Language for Control Systems, version 1.6*, INL Critical Infrastructure Protection/Resilience Center, Idaho Falls, USA, June 2006.
  On-line: http://www.msisac.org/scada/documents/12July07_SCADA_procurement.pdf

5.2 Security Awareness

- Steven S. Smith, *The SCADA Security Challenge: The Race is On*, November 25, 2006.
- NERC, *NERC Top 10 Vulnerabilities of Control Systems, version 2007,* March 2007.
  On-line: http://www.us-cert.gov/control_systems/pdf/ 2007_Top_10_Formatted_12-07-06.pdf

5.3 Information security and SCADA/process control

- E.M.M. Castelijn, J.G.J. Nijhuis, *Informatiebeveiliging Waterbedrijven (Information Security in Water Companies)*, VEWIN August 2004.
- N. Lammers, N.T.C. Zantkuyl, Update of *Informatiebeveiliging Waterbedrijven (Information Security in Water Companies)*, VEWIN, March 2007.

  Together, the publications above provide the Dutch drinking water sector with a set of guidelines for an across-the-board response to information security issues in the sector on the basis of the ISO/IEC 17799:2005 standard (Code of Practice for Information Security Framework). The document at hand provides the good practices for the process control environment.

- K. Stoffler, J. Falco & K. Kent, *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security*, NIST Special Publication SP800-82 (draft), USA, September 2006. On-line: http://csrc.nist.gov/publications/drafts/800-82/Draft-SP800-82.pdf

  Describes some of the same topics as the TNO/KEMA study and looks at a number of SCADA weaknesses. Ch. 5 contains information on correct firewall settings on the border of the PA environment. Ch. 6 contains SCADA-specific details for the Code of Practice for Information Security controls. The report contains an extensive list of literature and web references.

- ISA, *ISA-TR99.00.01-2007 -- Security Technologies for Industrial Automation and Control Systems, Instrumentation, Systems, and Automation Society*, (draft) Technical Report 2007. Note: this report will become IEC/TR 62443-5.

  Contains a set of technical SCADA security topics such as authentication and authorisation technology, firewalls and encryption, intruder detection technology, known weaknesses and recommendations for mitigation. The report is more detailed than the NIST SP800-82 report and contains an extensive list of literature and web references.

5.4 SCADA network security

- NISCC, *Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks*, 2005. See the website: http://www.cpni.gov.uk/ go to *Products and Services* and then go to Good Practices. Now select SCADA firewall guidance.
- DoE, *21 Steps to Improve Cyber Security of SCADA Networks, Office of Energy Assurance*, Office of Independent Oversight And Performance Assurance, U.S. Department of Energy, USA, 2005. On-line: http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf
- Luijf, H.A.M., *Slachtoffer van computercriminaliteit, wat dan?(A victim of computer criminality, what now?)*, 'Beveiliging' magazine, November 2007.
- ECP.NL/KWINT programme, *Voorlichtingsmateriaal (potentiële) computercriminelen (Information on (potential) computer criminals)*, 2005. On-line: http://www.ecp.nl/download/ Voorlichtingsmateriaal_tbv_(potentiële)_computercriminelen.pdf
- GovCert.NL, *Van herkenning tot Aangifte (From Detection to Reporting a Crime)*, The Hague, 2005. On-line: http://www.govcert.nl/render.html?it=39

5.5 SCADA web collections

- http://www.cpni.gov.uk
  Collection of SCADA Good Practice Guides intended primarily for management (click Products and Services, click Good Practices).
- http://www.us-cert.gov/control_systems/index.html
  A large number of documents and references about SCADA security.
- http://csrc.nist.gov/publications/
  A large number of Good Practices in sub-areas of system and network information security, including SCADA, firewalls, data carrier management, etc.

- http://www.thei3p.org/site_index/
  A large number of recent American research and good practice documents in the SCADA field from the Institute for Information Infrastructure Protection (I3P).
- http://www.scadasec.net/secwiki/ScadaSec
  Links to various SCADA papers, standardisation groups and other interesting SCADA sources.

5.6 American web sources for the water sector

- http://www.waterisac.org
  Links to a number of drinking water organisations, literature and background information.

6 References

[1] H.A.M. Luiijf, *Analyse SCADA-veiligheid in de Nederlandse drinkwatersector (Analysis of SCADA security in the Dutch drinking water sector)*, TNO Report, TNO-DV 2007 C317, July 2007. Classification: NICC Confidential.

[2] H.A.M. Luiijf and R. Lassche, *SCADA (on)veiligheid: een rol voor de overheid? (SCADA (in)security: a role for the government),* TNO-KEMA report, April 2006.

[3] ISO, Code voor Informatiebeveiliging/*Information technology - Security techniques - Code of practice for information security management framework*, ISO/IEC 17799:2005
Note: is soon to be renumbered to ISO/IEC 27002; the Dutch version was published as NEN-ISO/IEC 17799:2005.

[4] EWICS TC7: *A Study of the Applicability of ISO/IEC 17799 and the German Baseline Protection Manual to the Needs of Safety Critical Systems*.
European Workshop on Industrial Computer Systems - Executive Summary.
On-line: http://www.ewics.org/attachments/roadmap-project/ RdMapD31ExecSummary.pdf

[5] EWICS TC7: *A Study of the Applicability of ISO/IEC 17799 and the German Baseline Protection Manual to the Needs of Safety Critical Systems*.
European Workshop on Industrial Computer Systems.
On-line: http://www.ewics.org/attachments/roadmap-project/RdMapD31.pdf

[6] ISO, *Information technology -- Security techniques -- Information security management systems -- Requirements,* ISO/IEC 27001:2005.

[7] Gary Finco et al., *Cyber Procurement Language for Control Systems, version 1.6*, INL Critical Infrastructure Protection/Resilience Center, Idaho Falls, USA, June 2006.

[8] Department of Energy, *21 Steps to Improve Cyber Security of SCADA Networks*, Office of Energy Assurance, Office of Independent Oversight And Performance Assurance, U.S. Department of Energy, USA, 2005.
On-line: http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf

[9] *SCADA Security and Terrorism: We're not crying wolf.*
On-line: http://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf

[10] NERC, *Top 10 Vulnerabilities of Control Systems*, version 2007.
On-line:
http://www.us-cert.gov/control_systems/pdf/2007_Top_10_Formatted_12-07-06.pdf

[11] IEC, *Security for Industrial Process Measurement and Control - Network and system security*, (draft) report, IEC 62443:2007. Note: will be split into 5 parts.

[12] K. Stoffler, J. Falco, K. Kent, *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security*, NIST Special Publication SP800-82 (draft), USA, September 2006.

[13] ISA, *ISA-TR99.00.01-2007 -- Security Technologies for Industrial Automation and Control Systems, Instrumentation, Systems, and Automation Society*, (draft) Technical Report 2007. Note: will become IEC/TR 62443-5.

[14] ANSI/ISA-95.00.01-2000: Enterprise Control System Integration 1: Models and terminology. On-line: http://www.isa95.com

A Good Practices Checklist

Table A.1 SCADA Good Practices for the management team.

Main topic	Good Practice	√
Company security policy	#1 General information security policy linked with a specific SCADA security policy	
	#2 Code of Practice for Information Security and the associated security management system	
	#3 SCADA-specific policy is a logical extension of the general (information) security policy	
	#4 The SCADA security policy includes physical security	
	#5 Duties, responsibilities and authorisations laid down in writing	
Risk management	#6 SCADA risk is part of company level risk management	
Security awareness	#7 Continuous security awareness programme	
Audit	#8 At least one annual EDP audit of the SCADA environment	
Acquisition policy	#9 Disaster clause for acquisitions/contracts	
	#10 Security requirements are part of acquisition process	
	#11 Security clause in contracts for maintenance/work by third parties	

Table A.2 SCADA Good Practices for the technical PA management team.

Main topic	Good Practice	√
Defence in depth	#12 Principle of defence in depth	
Separate SCADA and OA environments	#13 Separated SCADA and office automation environments	
	#14 Guaranteed availability inn case of shared networks	
Secure links to the SCADA environment	#15 Removal of non-essential communication links	
	#16 Continuously monitored control of links	
	#17 Strictly configured and monitored firewalls	
	#18 No direct Internet link to the PA environment	
	#19 No use of the Internet for information transfer	
	#20 No wireless access points	
	#21 A strict regime for dial-up modems/external access	
	#22 Security measures and settings for the network separators and links are verified regularly	
Secure SCADA systems and network components	#23 Hardened/optimally secured systems	
	#24 Documented configurations	
	#25 Controlled configuration modification process	
	#26 Latest antivirus software	
	#27 Effective patch policy	
Secure protection of the SCADA environment	#28 Physical and electronic access control protection	
	#29 Connect only authorised equipment to the SCADA network	
	#30 Third party equipment is not connected unless under strict control	
Password policy for the SCADA environment	#31 Replace default passwords immediately before any use	
	#32 Essential passwords: complex, limited circle of users, replace regularly	
	#33 Personal passwords: strictly personal, replace regularly	
Business continuity measures	#34 According to Code of Practice for Information Security [3] Ch.14	
	#35 Regular back-up of SCADA systems and network components	
	#36 Secure remote storage of back-ups	
	#37 Regular verification of usability/completeness of back-up	
	#38 Maintained and practised continuity plan	
Management of information media	#39 Effective management and their controlled disposal	

TNO Defence, Security and safety

Author
Eric Luiijf MSc (Eng) Delft

TNO Defence, Security and Safety
P.O. Box 96864
2509 JG The Hague, The Netherlands

T: +31 70 374 0000
E: eric.luiijf@tno.nl
W: www.tno.nl

Published by
National Infrastructure against Cyber Crime (NICC)
A programme of the ICT Uitvoeringsorganisatie (ICTU)
P.O. Box 84011
2508 AA The Hague, The Netherlands

T: +31 70 888 7777
E: nicc@ictu.nl
W: www.ictu.nl

This is an English translation of the report:
SCADA Good Practice voor de Nederlandse Drinkwatersector,
TNO DV 2007 C478, December 2007
Translation by Language Unlimited B.V., Utrecht, The Netherlands

Cover photo: Oasen Drinkwater, by D. Van Eijndhoven

Publication Date: 25 February 2008