TNO Defensie en Veiligheid

Oude Waalsdorperweg 63
Postbus 96864
2509 JG Den Haag

www.tno.nl

T +31 70 374 00 00
F +31 70 328 09 61
info-DenV@tno.nl

TNO-rapport

TNO-DV 2007 C478

SCADA Good Practices voor de Nederlandse drinkwatersector

Datum	december 2007
Auteur(s)	ir. H.A.M. Luiijf
Opdrachtgever	NICC
Projectnummer	032.11460
Rubricering rapport	Ongerubriceerd
Titel	Ongerubriceerd
Samenvatting	Ongerubriceerd
Rapporttekst	Ongerubriceerd
Bijlagen	Ongerubriceerd
Aantal pagina's	33 (incl. bijlagen)
Aantal bijlagen	1

Managementuittreksel

Titel	:	SCADA Good Practices voor de Nederlandse drinkwatersector
Auteur(s)	:	ir. H.A.M. Luijf
Datum	:	december 2007
Opdrachtnr.	:	032.11460
Rapportnr.	:	TNO-DV 2007 C478

Probleemstelling
De SCADA Good Practices voor de Nederlandse drinkwatersector hebben tot doel de weerstand van de drinkwatersector tegen onbevoegde 'cyber'-beïnvloeding van de Supervisory Control and Data Acquisition (SCADA) en andere ICT in het procesautomatiseringsdomein sectorbreed op hoog peil te brengen. De beveiliging van die systemen en -netwerken in de Nederlandse drinkwatersector laat een divers beeld zien, zo blijkt uit eerdere analyse door TNO. Geconstateerd werd dat Nederlandse drinkwaterbedrijven op een aantal informatiebeveiligingsaspecten van het procesautomatiseringsdomein, soms onbewust, risico lopen.

Beschrijving van de werkzaamheden
In opdracht van het programma Nationale Infrastructuur Cybercrime (NICC), een programma van de ICT Uitvoeringsorganisatie (ICTU), heeft TNO Defensie en Veiligheid negenendertig SCADA Good Practices beschreven voor de drinkwatersector. Deze zijn gesplitst in onderwerpen die onder de verantwoordelijkheid vallen van het bedrijfsmanagementteam en in onderwerpen waarvoor het management van de technische procesautomatisering verantwoordelijk is.

Resultaten
Een goede beveiliging van de SCADA-omgeving, -systemen en -netwerken in de Nederlandse drinkwatersector is noodzakelijk om de leveringszekerheid en de kwaliteit van drinkwater in Nederland te garanderen, en te waarborgen dat de systemen niet onbevoegd gemanipuleerd kunnen worden. De te voorziene maatschappelijke effecten bij verstoring van de drinkwatervoorziening zijn te groot om het SCADA-risico niet onder controle te brengen. Denk bijvoorbeeld aan sociale onrust, gevolgen voor de volksgezondheid en grote economische schade.

Toepasbaarheid
De in dit rapport beschreven SCADA Good Practices geven sectorbreed handreikingen voor veilig SCADA-gebruik. Bij implementatie pakken ze de belangrijkste kwetsbaarheden aan die uit de eerdere analyse naar voren zijn gekomen. De beschreven SCADA Good Practices zijn gebaseerd op internationale standaarden, de-factostandaarden en succesvol toegepaste beveiligingsmaatregelen zoals die door andere bedrijven met SCADA worden toegepast.

Inhoudsopgave

Lijst met afkortingen

BCP	Business continuïteitsplanning
COTS	Commericial-Off-The-Shelf
CPNI	(VK) Centre for the Protection of National Infrastructure
DCS	Distributed Control Systems
DNP	Distributed Network Protocol
DoS	Denial-of-Service
EWICS	European Workshop on Industrial Computer Systems Reliability, Safety and Security
GPRS	General Packet Radio Service
HMI	Human-Machine Interface
ICT	Informatie- en Communicatietechnologie
IEC	International Electrotechnical Committee
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISA	Instrumentation Systems and Automation Society
ISO	International Organization for Standardization
LAN	Local Area Network
MAC	Media Access Control
MTU	Master Terminal Unit
NICC	Programma Nationale Infrastructuur Cybercrime
NISCC	(VK) National Infrastructure Security Co-ordination Centre (nu CPNI)
PA	Procesautomatisering
PLC	Programmable Logic Controller
POTS	Plain Old Telephony System
RTU	Remote Terminal Unit
TCP	Transmission Control Protocol
TNO	Nederlandse Organisatie voor toegepast natuurwetenschappelijk onderzoek
UMTS	Universal Mobile Telecommunication System
VEWIN	Vereniging van Waterbedrijven in Nederland
VPN	Virtual Private Network
WAN	Wide Area network

1 Inleiding

Procescontrolesystemen en -netwerken en meer in het bijzonder de Supervisory Control And Data Acquisition (SCADA) systemen en -netwerken[1], vormen een onmisbaar onderdeel in de keten van de leveringszekerheid en de kwaliteit van drinkwater in Nederland. Deze systemen meten, regelen en bewaken de volgende vitale processen:

- waterwinning en/of inname ruw water;
- transport van ruw water naar tussenbekkens en bezinkbekkens;
- transport naar de waterzuivering/filtratieprocessen;
- bewaken en besturen van waterzuivering en filtratieprocessen;
- monitoren en besturen van het kwaliteitscontroleproces;
- reinwaterdistributie, en
- aansturen van opvoerpompen.

Het Programma Nationale Infrastructuur Cybercrime (NICC) heeft in mei-juni 2007 een vragenlijst gebruikt om te inventariseren hoe de Nederlandse drinkwatersector de beveiliging van de procesautomatiseringsomgeving (PA) onder controle heeft.
Uit analyse [1] blijken er soms grote verschillen in de mate van SCADA-beveiliging te zijn tussen de drinkwaterbedrijven. Er is geconstateerd dat de drinkwaterbedrijven, soms onbewust, een risico lopen qua leveringszekerheid en kwaliteit van het drinkwater.
De SCADA-beveiliging is dus op een aantal punten voor verbetering vatbaar.
Om die reden is dit rapport met Good Practices voor de beveiliging van SCADA in de drinkwatersector opgesteld.

De opbouw van dit rapport is als volgt: hoofdstuk 2 bevat een korte achtergrond over wat SCADA is, welke toenemende dreigingen er zijn, en waar en waarom de proces-automatisering kwetsbaar is. Op basis van de sectorbrede analyse, internationale literatuur en standaarden worden in hoofdstuk 3 Good Practices aangereikt voor de managementteams van de drinkwaterbedrijven. De Good Practices zijn nadrukkelijk geen wetmatigheden, noch eisen. Drinkwaterbedrijven kunnen om goede redenen van interne cultuur of van organisatorische, architectonische of technische aard kiezen voor een geheel ander beveiligingsstelsel dat eenzelfde borging biedt. Desondanks is het goed om de hieronder beschreven Good Practices daartegen af te zetten, zodat geborgd wordt dat alle gaten in de beveiliging gedicht zijn. De Good Practices sluiten nauw aan bij de Code voor Informatiebeveiliging ([3], [6]), die in alle drinkwaterbedrijven als basis voor hun informatiebeveiliging in de kantooromgeving gebruikt wordt.
Bij het opstellen van de Good Practices is ook gekeken of de Good Practice al bij een of meer drinkwaterbedrijven in Nederland doorgevoerd is. Zo ja, dan geeft dat de mogelijk-heid voor drinkwaterbedrijven om in NICC- of ander verband bij hun concollega's na te gaan hoe zij die Good Practice hebben ingevoerd en wat de ervaringen daarmee zijn.
Hoofdstuk 4 bevat op vergelijkbare wijze de Good Practices voor het technisch PA-management. Hoofdstuk 5 geeft een aantal referenties naar SCADA-beveiligings-literatuur en -websites waar u meer informatie kunt vinden over specifieke deelonder-werpen. Hoofdstuk 6 bevat de literatuurreferenties en Appendix geeft twee checklists met de Good Practices.

[1] Aansluitend op het gebruik in de vakliteratuur wordt de term SCADA overkoepelend gebruikt voor alle vormen van procescontrolesystemen, tenzij specifiek ingegaan wordt op specifieke technologie.

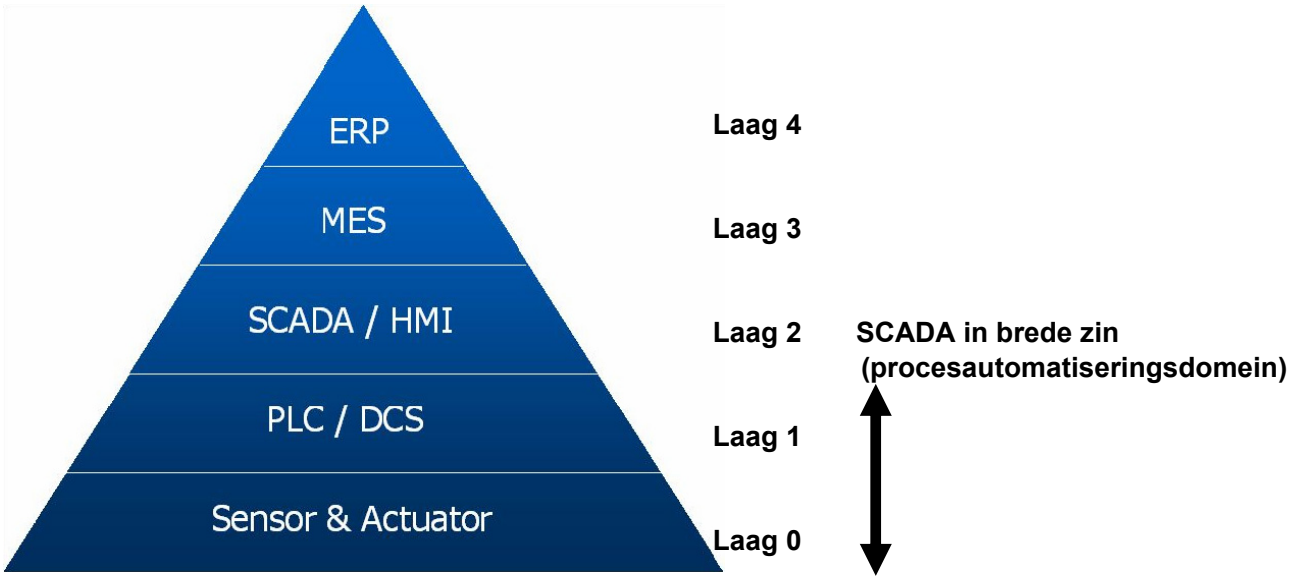
2 SCADA en SCADA veiligheid

In dit hoofdstuk wordt kort uitgelegd wat SCADA is, welke toenemende dreigingen er zijn, en waar en waarom de procesautomatisering kwetsbaar is. De inhoud van dit hoofdstuk is - met toestemming van het Ministerie van Economische Zaken - gebaseerd op het TNO-KEMA rapport '*SCADA (on)veiligheid: een rol voor de overheid?*' [2], waarin de SCADA informatiebeveiligingsproblematiek uitgebreid aan de orde komt inclusief een overzicht van nationale en internationale initiatieven en andere activiteiten op SCADA beveiligingsgebied.

2.1 Wat wordt verstaan onder de termen SCADA, PCS, DCS, RTU en PLC?

Het ISA-95 model [14] voor productiemodellering, onderscheidt voor procesautomatisering vijf hiërarchische niveaus in productie (zie figuur 1). Deze zijn:

- laag 0: de fysieke laag: sensoren, actuatoren en procesapparatuur;
- laag 1: Sensoroutput, commando's voor actuatoren en gecomputeriseerde besturing en bewaking (PLC);
- laag 2: Supervisory control laag (SCADA) en mens-machine interface (HMI);
- laag 3: Manufacturing Execution System (MES): het optimaal inzetten productiemiddelen, grondstoffen en mensen (resources) voor de productie (operations);
- laag 4: Business Planning en logistiek zoals Enterprise Resource Management, Supply Chain Management.



Figuur 1 ISA95-1 model voor productiemodellering

SCADA/HMI, de tweede laag van het model, verzorgt de volgende taken:

1 Visualisatie en bediening van procesonderdelen op verschillende plaatsen (mens-machine interactie).
2 Gecontroleerde gegevensuitwisseling met de procescontrolelaag, meestal PLC's.
3 Alarmmanagement, trend analyse en rapportage.
4 Loggen en opslaan van historische gegevens ('historian').
5 Afhandelen van batchoperaties – optioneel bij een SCADA pakket.
6 Gebruikersmanagement.

7 Analyse en bewerking van gegevens.
8 Gecontroleerde gegevensuitwisseling met de MES-laag / het administratieve domein.

Hierbij is het van belang te onderkennen dat elk van deze niveaus zijn eigen beveiliging kent. Dit rapport gaat echter in op de informatiebeveiliging van de onderste drie lagen en de uitwisseling van informatie met de hogere lagen.

De belangrijkste systeemcomponenten op de ISA95-1 lagen nul tot en met twee en hun functies worden hierna kort besproken. Een totaaloverzicht van de verschillende SCADA-systeemcomponenten en hun functies is te vinden in tabel 1. De lokale processors (PLC's) verzamelen meetgegevens van sensoren en besturen kleppen, afsluiters, motoren en dergelijke via hydroliek, pneumatiek en vermogenselektronica. Dergelijke lokale processors heten *Programmable Logic Controller* (PLC) als ze bestaan uit een processor op één elektronisch bord. Vaak worden er meer PLCs ingebouwd in één rek of behuizing. Een *Remote Terminal Unit* (RTU) is een lokale processor met meestal meer processorkracht dan een PLC die meer elektronicaborden aanstuurt. Voor de communicatie tussen de verschillende systemen worden meestal open communicatieprotocollen toegepast, zoals TCP/IP.

Voorbeeld
Via vloeistofsensoren of via een verschil in doorstroomsnelheid of druk (laag 0) constateert 'intelligentie' op laag 1 dat een pijpleiding lekt. Deze constatering kan vervolgens als een melding naar een centraal controlecentrum (laag 2) gestuurd worden. Daar wordt een alarm gegeven of wordt de onderhoudsploeg automatisch gewaarschuwd. Het alarm kan ook op een logische en georganiseerde manier op een operatorscherm getoond worden.

SCADA is een specifieke implementatie van procescontrolesystemen (PCS). Een andere op gedistribueerde besturing gebaseerde PCS-architectuur heet Distributed Control Systems (DCS) en omvat het volgen en controleren van meetinstrument tot bedieningsconsole. Procescontrolesystemen zijn normaal gesproken verspreid over grote afstanden en hebben soms voorgeprogrammeerde controlefuncties in het centrale computersysteem. DCS staan binnen op zich zelf staande grote faciliteiten waar de lokale processor zorgt voor de controlefuncties. Het onderscheid tussen SCADA- en DCS vervaagt echter steeds meer. Dat is mede de reden dat in de meeste vakliteratuur (en ook in dit document) de term SCADA generiek gebruikt wordt. De term SCADA (in brede zin) kan dan ook als het domein van procesautomatisering gezien worden.

Tabel 1 Terminologie en functies.

Component	Functies
Sensoren en instrumenten	Sensoren en instrumenten in het veld die condities detecteren zoals voltage, vermogen, druk, temperatuur, stroomsnelheid en klepstand.
Actuatoren	Actuatoren zoals pompen, kleppen, motoren en stroom- onderbrekers die op afstand of lokaal bediend kunnen worden.
Lokale processors	Lokale processors communiceren zowel met de sensoren en actuatoren als met functies in het netwerk. Ze kunnen enkele of alle van de onderstaande rollen vervullen: • Verzamelen van gegevens van de sensoren en instrumenten. • Het aan- of uitschakelen van de gekoppelde actuatoren door middel van interne (geprogrammeerde) logica, of gebaseerd op commando's verzonden door bedieningspersoneel of computers. • Vertalen van communicatieprotocollen zodat verschillende procescontrolesystemen en instrumenten met elkaar kunnen communiceren. • Identificeren van alarmcondities. Lokale processors worden momenteel onder verschillende namen gebruikt, zoals Programmable Logic Controller (PLC), Remote Terminal Unit (RTU), Intelligent Electronic Device (IED) en Process Automation Controller (PAC). Eén enkele lokale processor kan verantwoordelijk zijn voor het verzamelen van gegevens en het besturen van tientallen instrumenten en actuatoren.
Korte afstand communicatie-apparatuur	Korte afstand communicatieapparatuur zorgt voor de communicatie tussen de lokale processors en de sensoren en actuatoren. Over relatief korte kabels of draadloze connecties worden de analoge of digitale signalen gedragen.
Centraal Computersysteem	Het Centraal Computersysteem fungeert als het centrale controle- en besturingssysteem. Met behulp van dit systeem kan het bedieningspersoneel het proces controleren, alarmen ontvangen en bekijken, data analyseren, en besturingssignalen sturen naar actuatoren. In sommige gevallen bevat dit systeem geprogrammeerde logica om automatisch de lokale processors aan te sturen. In andere gevallen is dit systeem alleen een interface tussen het bedieningspersoneel en de lokale processors. Andere taken van het centrale computersysteem zijn het opslaan van meetgegevens en systeemtoestanden in een (historical) database en het genereren van rapportages. Het centrale computersysteem kan ook bekend staan als Master Terminal Unit (MTU) of de SCADA-server. In een aantal gevallen is het gewoon een personal computer (PC) met Human-Machine Interface software (HMI).
Lange afstand communicatie-apparatuur	Lange afstand communicatieapparatuur zorgt voor de communicatie tussen de lokale processors en het centrale computersysteem. Het netwerk strekt zich uit over afstanden van vele kilometers. Er wordt gebruik gemaakt van vaste huurlijnen, xDSL, dark fibre, satelliet, microgolf, punt-punt verbindingen, GSM, GPRS, UMTS en frame relay.

2.2 SCADA-gebruik in de drinkwatersector

SCADA-systemen en –netwerken (in brede zin) of te wel procesautomatisering (PA) vormen een onmisbaar onderdeel in de keten van de leveringszekerheid en de kwaliteit van drinkwater in Nederland. Deze systemen meten, regelen en bewaken (integrale alarm- en event-afhandeling) zowel lokaal als op afstand de volgende vitale drinkwater-processen:

- waterwinning en/of inname ruw water;
- transport van ruw water naar tussenbekkens en bezinkbekkens;
- transport naar de waterzuivering/filtratieprocessen;
- bewaking en besturing waterzuivering en filtratieprocessen;
- het kwaliteitscontroleproces;
- reinwaterdistributie, en
- aansturing van opvoerpompen.

Denk hierbij aan de bewaking en het regelen van de stroomsnelheid in leidingen, de druk in opslagtanks, het aan- of uitzetten van pompen, het regelen van afsluiters en het bewaken van de kwaliteitsaspecten van het water zoals pH-waarde en de troebelheid. Het alarmdisplay en mogelijkheden om in te grijpen zijn veelal geconcentreerd in een besturings- en bewakingscentrum. In de drinkwatersector staat dit vaak bekend als ‘centrale wacht’.

2.3 SCADA onveiligheid en het risico

De toenemende mate van onveiligheid van SCADA-systemen en –netwerken komt voort uit een aantal technische en organisatorische ontwikkelingen. Allereerst komt SCADA voort uit de klassieke omgeving van procesautomatisering met rekken vol elektronica en relais. Een omgeving waarin informatiebeveiliging geheel geen rol speelde. Dat was ook niet nodig omdat de SCADA-systemen en -protocollen gebaseerd waren op:

- gesloten leverancierеigen protocollen, technieken en onderliggend besturings-systeem (‘proprietary’);
- geen openbaarheid van informatie over de werking van SCADA;
- geen telecommunicatie dan wel alleen punt-puntverbindingen via vaste lijnen;
- geen koppelingen met de administratieve bedrijfsnetwerken en het Internet;
- implementaties zonder adequate beveiligingsmechanismen omdat uitgegaan wordt van hackervrije omgevingen;
- protocolimplementaties die geen rekening houden met ‘stresscondities’ zoals die kunnen optreden bij netwerkoverbelasting;
- systemen die niet gepatcht behoeven te worden;
- geheel gecontroleerde en afgesloten beveiligde omgevingen.

De hedendaagse praktijk is anders. Al de genoemde uitgangspunten zijn inmiddels achterhaald. Helaas blijkt vaak dat noch de toegepaste SCADA-techniek, noch de operationele omgeving qua informatiebeveiliging meegegroeid zijn met de snelle operationele en technische ontwikkelingen:

- De SCADA-protocollen zijn open standaard geworden; hun beschrijving is op het Internet te vinden.
- SCADA draait als toepassing boven op Windows of Linux en gebruikt Internet-protocollen (TCP/IP) voor het transport van gegevens. De kwetsbaarheden van die

systemen en protocollen zijn wereldwijd bij hackers bekend en kunnen uitgebuit worden met zogenaamde ‘toolkits’.
- De huidige mens-machine interface vergt geen moeilijk te leren commando’s meer, maar is gebaseerd op een webbrowser interface.
- Bedrijfsmatig is het noodzakelijk om koppelingen met bedrijfsnetwerken en openbare netwerken te maken. Er zijn ook modemtoegangen tot het SCADA-netwerk voor de besturing van thuis uit en voor onderhoud door leveranciers (zie ook [1]).
- Hackers en anderen raken er steeds meer geïnteresseerd in om in te breken op SCADA-systemen en -netwerken.
- Eenvoudige testen laten zien dat SCADA-systemen in de stress raken of zelfs geheel uitvallen zodra er een onbekend pakket via het netwerk naar toegestuurd wordt.
- Nieuwe, soms niet uit te schakelen, functionaliteit op PLC-borden zijn ingebouwde webservers waarmee van afstand op gebruiksvriendelijke wijze alle parameterinstellingen te wijzigen zijn.
- SCADA-apparatuur bevat soms standaard ingebouwde modems voor toegang door de leverancier.
- Wachtwoorden worden nooit gewijzigd en zijn niet persoonlijk; de omgeving is toch gesloten nietwaar?

Dit alles volstrekt zich in een procesautomatiseringsomgeving die zich nauwelijks bewust is van het SCADA-risico (zie ook de verschillende ‘examples’ in [9]). In de procesautomatiseringsomgeving is meestal een geheel andere cultuur aanwezig dan die binnen de bedrijfsautomatisering, waar informatiebeveiliging meer aandacht krijgt en beveiligingen tegen hackers, virussen, Trojaanse code en spam inmiddels gemeengoed zijn [10]. Daarnaast zijn de organisaties die procesautomatisering toepassen niet meegegroeid met de ontwikkelingen op het gebied van beveiliging van de procesautomatisering. Beveiliging is niet ingebed in het werkproces.en veelal is niet bekend wie de proceseiegenaar is.

Dat dit binnen de SCADA/procesautomatiseringsomgeving van de drinkwaterbedrijven op een aantal aspecten niet anders is, blijkt uit een aantal van de ‘rode’ en ‘gele’ vlaggen in [1]:
- er ontbreekt veelal een SCADA-specifiek beveiligingsbeleid;
- er wordt nog nauwelijks aan beveiligingsbewustwording gedaan;
- er worden voor onderkende risicofactoren (‘waar ligt de sector wakker van’) geen risicobeperkende maatregelen getroffen;
- derden kunnen zonder toezicht apparatuur op het SCADA-netwerk aansluiten;
- er vinden nauwelijks virus- en wormcontroles plaats; en
- noodzakelijke patches worden niet of laat aangebracht.

Tabel 2 Nog meer misvattingen over SCADA-onkwetsbaarheid.

Veronderstelling	Realiteit
We gebruiken gehuurde communicatielijnen, dus niemand heeft toegang tot onze communicatieverbindingen	Het is gemakkelijk om deze communicatielijnen af te tappen. (zie bijv. www.tscm.com/outsideplant.html).
We gebruiken inbelverbindingen en niemand weet de telefoonnummers	Een tap op de uitgaande lijnen of de gespecificeerde telefoonrekening geeft snel inzicht in alle nummers die gebeld zijn. Er bestaat 'war dialer' software waarmee automatisch nummerreeksen gebeld kunnen worden en die de nummers identificeren waarachter een modem zit.
We gebruiken terugbelmodems dus ongeautoriseerden kunnen geen toegang krijgen.	Op het moment dat een verbinding afgetapt kan worden is ook het terugbelmechanisme eenvoudig te verslaan. En er zijn methoden bekend waarmee niet eens een tap nodig is.
Onze systemen op afstand worden beveiligd door wachtwoorden.	De methoden om wachtwoorden te stelen zijn algemeen bekend. De eenvoudigste methode is om met een sniffer het verkeer af te luisteren. Hiermee kan het wachtwoord onderschept worden wanneer dit in normale tekst over de communicatielijn gaat. Wachtwoordgokmethoden met behulp van een woordenboek zijn ook algemeen bekend. Het uitwisselen van wachtwoorden of deze nooit wijzigen is heel gebruikelijk. Te vaak worden er ook zeer simpele wachtwoorden met een beperkt aantal tekens gebruikt en nooit gewijzigd.
We gebruiken frequentiemodulatie-technieken, dezelfde die militairen ook gebruiken voor beveiligde communicatie.	Er zijn simpele methoden om frequentiemodulatie reeksen te decoderen. De Wireless LAN Associatie raadt ook aan om op alle netwerken versleuteling te gebruiken, ook op de frequentiemodulatienetwerken.
We gebruiken een protocol dat alleen bekend is bij enkelen buiten de leverancier; indringers kunnen onze SCADA-berichten niet begrijpen.	Zelfs de protocollen die eigendom zijn van bepaalde leveranciers zijn meer algemeen bekend dan de meesten zich realiseren. Leveranciers, consultants, huidige en ex-werknemers van zowel het eigen als andere bedrijven die hetzelfde SCADA-protocol gebruiken, kennen alle details. Handleidingen en software voor het analyseren van de protocollen kunnen op het Internet gevonden worden.

2.4 Incidenten met SCADA in de drinkwater- en andere sectoren

De dreigingen voor de procesautomatisering vallen uiteen in:

- Organisatorische bedreigingen, denk bijvoorbeeld aan gebrek aan beveiligings-beleid, gebrek aan aandacht voor beveiligingsbewustzijn, slecht gereguleerde toegang tot de systemen, geen wachtwoordbeleid, en dergelijke.
- Fysieke bedreigingen, denk aan explosie of brand of vernietiging door vandalen.
- Technische bedreigingen, denk bijvoorbeeld aan sofware- en hardwarestoringen, virussen, denial-of-service aanvallen.

Wereldwijd worden incidenten met SCADA nauwelijks gepubliceerd. Als ze al gepubliceerd worden, dan is dat vaak buiten Europa. Europese bedrijven houden de incidenten graag achter of melden alleen een 'technische storing'. In [2] staat een lijst met openbaar gemaakte incidenten met SCADA-systemen in een aantal sectoren. Slechts een beperkt aantal incidenten zijn internationaal vanuit drinkwaterbedrijven bekend gemaakt. In Nederland heeft in ieder geval één beveiligingsincident zich voorgedaan.
Hieronder een aantal van de openbaar gemaakte incidenten in de drinkwatersector:

- **Manipulatie drinkwater- en rioolwaterzuiveringsinstallaties, Australië**
  Het voorbeeld dat het meest wordt aangehaald om de kwetsbaarheid van SCADA-systemen en –netwerken aan te tonen is dat van de ongeautoriseerde toegang tot het procescontrolesysteem van de drinkwater- en rioolwaterzuiveringsinstallaties van Hunter Watertech in Maroochy Shire, Australië door de ex-contractant Vitek Boden.
  Boden was opzichter die de SCADA-systemen installeerde voor Hunter Watertech. Het SCADA-systeem bevatte een locale processor bij elk van de meer dan 300 pompstations. Iedere lokale processor communiceerde met het centrale computersysteem via een radioverbinding. Na twee jaar gewerkt te hebben aan dit project, was het project eind 1999 bijna gereed. Boden nam ontslag en vroeg Hunter Watertech naar werkmogelijkheden. Deze nam hem niet aan. Korte tijd later begonnen pompstations van het rioleringssysteem storingen te vertonen en vielen kleppen dicht in het drinkwatersysteem.
  Tijdens een politiecontrole op 23 april 2000 ontdekte de politie een PC en radio-zendapparatuur in de auto van Vitek Boden. Die gaf daarop toe de SCADA-systemen van Hunter Watertech 46 keer op afstand gemanipuleerd te hebben. Hij schakelde alarmmeldingen uit, verstoorde communicatie, liet pompen niet op de juiste tijd aanslaan en zorgde voor het via overstorten laten vrijkomen van ongezuiverd afvalwater. Naar schatting is tussen januari 2000 en 23 april 2000 bijna een miljoen liter ongezuiverd rioolwater vrijkomen in het milieu.[2]
- **Vernieling SCADA-systeem in Tshwane, Zuid Afrika**
  Op 18 augustus 2006 vernielden vandalen het SCADA-systeem van een reservoir in Tshwane, Zuid Afrika. Het resultaat was dat Mamelodi en Eersterust (Pretoria) gedurende elf dagen geen drinkwateraanvoer hadden.
- **Hacker in drinkwaterfiltratiesysteem, Harrisburg, Pennsylvania, VS**
  Een hacker dringt door tot de SCADA van het drinkwaterfiltratiesysteem van de drinkwatervoorziening in Harrisburg, Pennsylvania, VS. Hij doet dit door de overname op afstand van de laptop van een medewerker van het drinkwaterbedrijf nadat deze Trojaanse code had geïnstalleerd. Zodra deze medewerker telewerkend aanlogde, kon de hacker van uit het Internet via de laptop het SCADA-netwerk penetreren. Daarna installeerde de hacker 'malware' (Trojaanse software) en spyware op de SCADA-systemen. Daarmee kon de indringer in principe het SCADA-netwerk overnemen, valse commando's geven en het netwerk volledig overbelasten.[3]
- **Communicatieprobleem drinkwaterdistributiesysteem, Fort Worth, VS**
  Communicatieproblemen met de decentrale SCADA-systemen leidden tot een achturige uitval van een deel van de drinkwatervoorziening in Forth Worth op 14 januari 2007. Men was de gehele controle over pompen en voorraadtanks kwijt.

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

- **Hackerpenetratie drinkwatersysteem, VS**
  De Amerikaanse Water-ISAC rapporteerde dat in 2000 een SCADA-systeem van een drinkwaterbedrijf gepenetreerd is door hackers.
- **Softwarefout in SCADA** zorgt voor een te laag chloorniveau wat het drinkwater onbruikbaar maakt in Lewiston MA, VS (2003).

Gepubliceerde incidenten met SCADA-systemen in andere sectoren zijn voorbeelden van de eerder in paragraaf 2.3 genoemde SCADA-onveiligheden:
- De zwakke en vaak niet-beveiligde SCADA-protocollen waardoor systemen falen.
- Zwak of onbeveiligde communicatieverbindingen met bedrijfsnetwerken en de buitenwereld waardoor hackers en virussen door kunnen dringen.
- Onderhoudsleveranciers die ingestelde beveiligingen kunnen omzeilen door gebrekkig toezicht op welke apparatuur aangesloten mag worden (zelfs in een kerncentrale).
- Gebrek aan wijzigingsbeheer.
- Gebrek aan fysieke afscherming en beveiliging van de SCADA-systemen en -netwerken.

> 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 Noodzaak voor SCADA-beveiliging in de drinkwatersector

Een goede beveiliging van de SCADA-omgeving, -systemen en -netwerken (lagen 0 tot en met 2 uit figuur 1) in de Nederlandse drinkwatersector is noodzakelijk om de leveringszekerheid en de kwaliteit van drinkwater in Nederland te garanderen en om te waarborgen dat de SCADA-systemen niet onbevoegd gemanipuleerd kunnen worden. Bovengenoemde hackerproblemen, virussen en verlies van communicatie tussen SCADA-netwerkdelen kunnen ook in Nederland optreden.
De te voorziene maatschappelijke effecten daarvan echter groot, denk bijvoorbeeld aan maatschappelijke gevolgen als sociale onrust, gevolgen voor de volksgezondheid en grote economische schade.

De vitale drinkwaterbedrijven dienen daarom het SCADA-risico, als onderdeel van het totale bedrijfsrisico, onder controle te hebben. Uit [1] blijkt dat dit sectorbreed nog niet het geval is.

Samengevat kan geconcludeerd worden, dat een goede beveiliging van SCADA-systemen en -netwerken noodzakelijk is. Deze beveiliging vraagt om een aanpak waarbij gebalanceerd aandacht wordt besteed aan zowel de organisatorische, fysieke en systeem- en netwerktechnische aspecten van informatiebeveiliging. De hierna volgende Good Practices voor SCADA geven daarbij een handreiking voor het managementteam en het technisch procesautomatiseringsmanagement.

3 Good Practices voor het managementteam

Om binnen de drinkwatersector op goede wijze het hoofd te bieden aan de hiervoor beschreven SCADA-risicoaspecten wordt u in dit document een aantal Good Practices aangereikt. Good Practices zijn nadrukkelijk geen wetmatigheden, noch eisen. Drinkwaterbedrijven kunnen om goede redenen van organisatorische, architectonische, technische of interne cultuur aard kiezen voor een geheel ander beveiligingsstelsel dat eenzelfde borging biedt. Desondanks is het goed om de in dit document beschreven Good Practices daartegen af te zetten, zodat geborgd wordt dat alle gaten in de beveiliging gedicht zijn.

De Good Practices zijn ondergebracht in twee groepen. Als eerste de in dit hoofdstuk opgenomen Good Practices op bedrijfsmanagementniveau. In het volgende hoofdstuk zijn de Good Practices op het technische procesautomatiseringsniveau te vinden.

De onderstaande Good Practices op bedrijfsmanagementniveau bouwen voort op het algemene informatiebeveiligingsbeleid zoals dat in de drinkwaterbedrijven aanwezig is en sluiten aan bij de algemene bedrijfscultuur van risicobeheersing. De Good Practices zijn geclusterd onder de volgende hoofdonderwerpen:

- Bedrijfsbeveiligingsbeleid en specifiek SCADA-beveiligingsbeleid.
- Risicomanagement.
- Audit.
- Verwervingsbeleid SCADA-systemen, -netwerken en -diensten.

3.1 Bedrijfsbeveiligingsbeleid en specifiek SCADA-beveiligingsbeleid

Een juiste inpassing van informatiebeveiliging voor SCADA-systemen en –netwerken vereist een omgeving waarin managementaandacht bestaat voor beveiliging. Het gaat hierbij om beleid ingebed in het bedrijfsproces op basis van risicoanalyse en een drinkwaterbedrijfsbreed risicomanagementproces.

Good Practice 1
Het drinkwaterbedrijf heeft een algemeen informatiebeveiligingsbeleid met daaraan gekoppeld een specifiek SCADA-beveiligingsbeleid.

Good Practice 2
Het algemene informatiebeveiligingsbeleid is gebaseerd op de Code voor Informatie-beveiliging [3] en het bijbehorende managementsysteem [6].[4]

Good Practice 3
Uitgangspunt voor het specifieke SCADA-beveiligingsbeleid is dat dit op een dusdanige wijze geïmplementeerd kan worden dat getroffen maatregelen voor de medewerkers een logisch verlengde vormen van het algemene (informatie)beveiligingsbeleid en de beveiliging van de kantooromgeving (KA).

[4] Noot: de beveiligingsmonitor van de VEWIN en de Amsterdamse Gemeentelijke InformatieBeveiligings Norm (GIBN) zijn afgeleid van de Code voor Informatiebeveiliging.

Good Practice 4
Het specifieke SCADA-beveiligingsbeleid omvat tevens de fysieke beveiliging van de SCADA-systemen en -netwerken.

Good Practice 5
Voor de SCADA-omgeving zijn de beveiligingsverantwoordelijkheden, -taken en -bevoegdheden voor functionarissen en de gebruikers van SCADA vastgesteld (zie ook [8] punt 12).

Achtergrond
- In de Amerikaanse Top-10 van SCADA-kwetsbaarheden [10] staat het gebrek aan SCADA-specifiek beveiligingsbeleid, beveiligingsprocedures en beveiligingscultuur aan de top.
- Gebrek aan een informatiebeveiligingsbeleid en gebrek aan een risicoanalyse leidt tot het ad hoc treffen van beveiligingsmaatregelen. Daardoor is het nooit duidelijk of de juiste beveiligingsmaatregelen getroffen zijn en welke beveiligingsgaten er zijn.
- Binnen het informatiebeveiligingsbeleid volgens de Code voor Informatiebeveiliging zijn een aantal beheersmaatregelen (controls) opgenomen die niet direct passen bij de praktijk van de 24-uurs SCADA-omgeving. Volgens [4] en [5] vereist een aantal in de Code voorkomende borgingelementen enige aanvulling. De belangrijkste elementen zijn: uitbesteding, afstemming informatiebeveiliging en procesveiligheid, fysieke beveiliging van de ICT-omgeving (lees SCADA-omgeving), operationele procedures (24 uur), antivirusbeleid, logging en alarmering, toegangscontrole, wachtwoordbeleid (zie ook paragraaf 4.6) en bedrijfscontinuïteitsmanagement. Om die reden is het aan te bevelen om een aparte beleidsaanvulling te ontwikkelen. Ook is het verstandig dat er een duidelijke rapportagelijn is voor het melden van geconstateerde beveiligingsincidenten (zie ook Code voor Informatiebeveiliging [3], paragraaf 11.2).
- Elementen die het 'levende' en dus regelmatig onderhouden SCADA-beveiligingsbeleidsdocument bevat zijn duidelijke en begrijpbare van de bedrijfsdoelstellingen (leveringszekerheid en kwaliteit van drinkwatervoorziening) afgeleide beveiligingsdoelstellingen, beveiligingsorganisatie, regels en procedures. Wat zijn de rollen en verantwoordelijkheden van specifieke functies en van de overige medewerkers die betrokken zijn bij de procesautomatisering (PA) of daarmee werken? Wat is expliciet niet toegestaan en wat wordt van de medewerker of functionaris verwacht bij constatering van een (potentieel) beveiligingsincident?

Status: Het merendeel van de drinkwaterbedrijven hanteert een informatiebeveiligingsbeleid dat gebaseerd is op de Code voor Informatiebeveiliging [3]. Volgens [1] hebben echter nog niet alle drinkwaterbedrijven een informatiebeveiligingsbeleid en heeft de helft van de drinkwaterbedrijven geen specifiek SCADA-beveiligingsbeleid.

3.2 Risicomanagement

Good Practice 6
De procesautomatisering/SCADA-omgeving vormt een integraal onderdeel van het risicomanagementproces op het allerhoogste bedrijfsniveau.

Achtergrond: De procesautomatisering/SCADA-omgeving is een essentieel onderdeel van het bedrijfsproces dat zorgt voor de leveringszekerheid en kwaliteit van het drinkwater.

De veiligheid in al haar aspecten (beschikbaarheid, betrouwbaarheid, vertrouwelijkheid) van de SCADA-systemen en -netwerken, de risicoanalyse, het risicomanagement en de bijbehorende business continuïteitsplanning (BCP) zijn daarop afgestemd.

Status: Binnen de meeste drinkwaterbedrijven worden de risicofactoren verbonden aan SCADA-systemen en –netwerken nog niet expliciet betrokken in het bedrijfsbrede risicomanagementproces ondanks hun cruciale rol in de leveringszekerheid en de kwaliteit van drinkwater.

3.3 Beveiligingsbewustwording

Een van de grootste intern te beheersen risicofactoren is de menselijke factor. Ook in de SCADA-omgeving vormt dit een grote risicofactor. Beveiligingsbewustwording helpt om de beveiligingsattitude van het management (voorbeeldfunctie) en de medewerkers scherp te krijgen en het beveiligingsniveau van de organisatie te verbeteren.

Good Practice 7
Het drinkwaterbedrijf heeft een doorlopend beveiligingbewustzijnsprogramma.

Achtergrond: Goede informatiebeveiliging vereist continu aandacht voor het beveiligingsbewustzijn en de beveiligingsattitude van de medewerkers, zeker daar waar het de vitale bedrijfsprocessen betreft. Als de eigen medewerkers geen bewuste beveiligingsattitude hebben, zullen ze dat ook uitstralen naar derden (leveranciers, onderhouds- en storingstechnici) die aan de SCADA-systemen of -netwerken moeten werken. Hiermee wordt het potentiële risico van onbewuste of bewuste ongewenste beïnvloeding van de SCADA-systemen en daarmee het drinkwaterproces vergroot. (zie ook [8] punt 21).

Status: Volgens [1] besteedt de helft van de drinkwaterbedrijven geen aandacht aan de beveiligingsbewustwording en -attitude van de SCADA-medewerkers.

3.4 Audit

Good Practice 8
Minimaal eenmaal per jaar wordt een EDP-audit van de SCADA-systemen en -netwerken uitgevoerd.

Achtergrond: Het Burgerlijk Wetboek deel 2, Artikel 393 over de Jaarrekening stelt: '*De accountant brengt omtrent zijn onderzoek verslag uit aan de raad van commissarissen en aan het bestuur. Hij maakt daarbij ten minste melding van zijn bevindingen met betrekking tot de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking.*'

Dit wetsartikel is onderdeel van de Wet Computercriminaliteit I. De achtergrond van deze extra opdracht aan de accountant is de volgende. Ingeval van een daad van computervredebreuk, computerterreur, of andere vorm van computercriminaliteit, kan een opgespoorde en vervolgde dader in de rechtbank ter verdediging stellen dat hij/zij niet wist dat hij/zij inbrak, dat er geen enkele beveiliging was waardoor hij/zij zich zomaar in een systeem of netwerk bevond, enzovoorts. De advocaat van de dader(s) kan eisen dat uw bedrijf aantoont dat er voldoende beveiligingen zijn aangebracht, kortweg 'geeft u al uw beveiligingsplannen en details' aan de rechtbank en daarmee aan de

openbaarheid prijs. Reden voor de meeste bedrijven om dan maar geen aangifte te doen en geen inzage te geven, waarmee de dader of daders meestal vrij uitgaan.

De accountantsverklaring in het kader van de jaarrekening - indien aanwezig *en in uw geval aantoonbaar ook de SCADA-systemen en -netwerken omvattende* - is volgens het Burgerlijk Wetboek afdoende om aan te tonen dat u voldeed aan de wettelijke vereisten van '*enige mate van beveiliging*' die de verdachte willens en wetens doorbroken heeft. Detailgegevens over de beveiliging behoeven dan niet overhandigd te worden. Het risico van het niet hebben van een accountantsverklaring in het kader van de jaarrekening die de SCADA-netwerken expliciet omvat is dus dat een vervolging van de daders aanzienlijk moeilijker wordt met het risico dat bedrijfsgevoelige beveiligingsmaatregelen op straat komen te liggen.

In de audit komt in ieder geval aan de orde:
- Wachtwoord- en toegangsbeleid.
- De veiligheid van de verbindingen tussen enerzijds de SCADA-systemen en -netwerken en anderzijds kantoorautomatisering, publieke netwerken en het Internet (zie ook [8] punten 9 en 18).
- De beveiligingsstatus van op afstand bewaakte en geregelde locaties (zie ook [8] punt 10).
- Eventuele modemtoegangen.
- De wijze van rapportage van beveiligingsincidenten, beveiligingslogging en de opvolging daarvan.
- De fysieke en elektronische beveiliging van de SCADA-systeemcomponenten en -netwerken (zie ook [8] punten 10 en 18), zoals sloten op behuizingen, alarmen op deuren en dergelijke.

Naast een formele audit is het aan te bevelen om enkele malen per jaar een interne beveiligingsaudit uit te voeren welke gesynchroniseerd kan worden met stappen van het beveiligingsbewustzijnsprogramma.

Status: Volgens [1] heeft driekwart van de drinkwaterbedrijven dit niet geregeld.

3.5 Verwervingsbeleid SCADA-systemen, -netwerken en -diensten

Informatiebeveiliging omvat de gehele levenscyclus van SCADA-apparatuur, -programmatuur en -diensten. Verwerving is een belangrijke stap waarin de interne beveiligingseisen aan leveranciers en andere derden duidelijk vastgelegd kunnen worden. Het helpt ook om de externe partij duidelijk te maken dat het drinkwaterbedrijf beveiliging professioneel en serieus aanpakt.

Good Practice 9
In de met leveranciers af te sluiten contracten voor (grote) SCADA-systemen en –netwerken wordt een continuïteitsparagraaf opgenomen met als doel de leverings-zekerheid en de kwaliteit van drinkwater te borgen:
1 De leverancier garandeert voor een af te spreken aantal jaren dat er voldoende reservecomponenten op voorraad zijn.
2 De leverancier garandeert dat deze bij calamiteiten ondersteuning biedt om een oplossing te vinden.

3 In geval het SCADA-systeem en/of –netwerk door wat voor oorzaak ook teloor gaat, verleent de leverancier met voorrang medewerking aan de vervanging van het SCADA-systeem en/of -netwerk.
4 De leverancier verifieert patches van derden die essentiële systeemdelen leveren (bijvoorbeeld Microsoft besturingssysteem) binnen een korte doorlooptijd en stelt deze daarna op een vertrouwde wijze beschikbaar.

Achtergrond: Om de leveringszekerheid en de kwaliteit van drinkwater te borgen dienen de SCADA-systemen die de vitale drinkwaterprocessen monitoren en besturen zowel bij een gewone storing als bij een calamiteit zo snel mogelijk weer functioneel te zijn.

Status: Volgens [1] heeft de helft van de drinkwaterbedrijven dergelijke calamiteiten-afspraken met de leverancier gemaakt.

Good Practice 10
Het drinkwaterbedrijf stelt voorafgaande aan de verwerving eisen voor informatie-beveiliging op waaraan de te verwerven SCADA-systemen, -netwerken en -program-matuur moeten voldoen. Zie ook de Code voor Informatiebeveiliging [3], hoofdstuk 12.

Achtergrond: Daar een SCADA-systeem en –netwerk vaak als integraal project geïntroduceerd wordt, is het belangrijk om vooraf geregeld te hebben aan welke beveiligingseisen het op te leveren systeem moet voldoen. In [7] is een aanzet te vinden voor technische eisen. Leg ook vast dat de leverancier niet zonder expliciete toestemming aan derden bekend mag maken dat zij SCADA-systemen aan het drinkwaterbedrijf heeft geleverd.

Status: De helft van de drinkwaterbedrijven besteedt geen aandacht aan eisen voor informatiebeveiliging tijdens de verwervingsfase van SCADA-apparatuur en -program-matuur.

Good Practice 11
In de met derden voor onderhoud en ondersteuning af te sluiten contracten wordt een beveiligingsparagraaf opgenomen.

Minimaal wordt daarin het volgende geregeld:
1 Het conformeren door onderhouds- en ondersteuningstechnici van derden aan het vigerende bedrijfsbeveiligingsbeleid voor de SCADA-systemen en – netwerken.
2 Clearance-afspraken en toegangsafspraken voor onderhoudstechnici.
3 Garanties m.b.t. de bescherming van de vertrouwelijke bedrijfsinformatie (zie ook [8] punt 21).
4 Toezicht door het drinkwaterbedrijf op de door de derde te verrichten werkzaamheden.
5 Afvoer van (defecte) informatiedragers met daarop eventuele bedrijfsgevoelige informatie.

Achtergrond: Het vigerende bedrijfsbeveiligingsbeleid voor de SCADA-systemen en -netwerken omvat ook de medewerkers van derden. Als eerste geldt voor hen dat de toegang tot de SCADA-systemen restrictief is. Minimaal zijn er garanties vanuit de derde dat haar medewerkers vertrouwd kunnen worden (bijvoorbeeld door aansprakelijkheid derde voor alle acties van zijn medewerkers, Verklaring Omtrent Gedrag (VOG), enzovoort) De condities waaronder apparatuur en programmatuur van de derde (onder andere laptop onderhoudstechnicus, modem) aan de SCADA-systemen of -netwerk

aangesloten mag worden, zijn afgesproken en vastgelegd. Alle handelingen door derden aan systemen en netwerkcomponenten in de SCADA-omgeving gebeuren onder toezicht. Dit voorkomt dat ernstige verstoringen optreden waardoor de leveringszekerheid van het drinkwater in gevaar komt (zie ook [8] punt 7). Afwijking van de procedure mag bijvoorbeeld alleen met toestemming van de beveiligingsfunctionaris.

Defecte informatiedragers en informatiedragers die ingebed zijn in te vervangen SCADA-systemen (bijvoorbeeld geheugens) kunnen bedrijfsgevoelige gegevens bevatten. Geregeld is dat dergelijke informatie het drinkbedrijf niet verlaat voordat zeker is gesteld dat de gevoelige informatie afdoende verwijderd of vernietigd is.

Status: De helft van de drinkwaterbedrijven heeft geen specifieke SCADA-beveiligingsafspraken vastgelegd in contracten met derden [1]. De regulering van de toegang door derden als onderhouds- en ondersteuningstechnici tot de SCADA-systemen en -netwerken is niet bij alle drinkwaterbedrijven een continu beheerst proces.

4 Good Practices voor het technisch PA-management

De Good Practices zijn geclusterd onder de volgende hoofdonderwerpen:
- Gelaagde bescherming.
- Gescheiden SCADA- en kantoorautomatiseringsomgevingen.
- Veilige koppelingen met de SCADA-omgevingen.
- Veilige SCADA-systemen en –netwerkcomponenten.
- Veilige afscherming van de SCADA-omgeving.
- Wachtwoordbeleid voor de SCADA-omgeving.
- Bedrijfscontinuïteit van de SCADA-systemen en –netwerkcomponenten.
- Beheer informatiedragers in de SCADA-omgeving.

Voor de opgestelde Good Practices is gebruik gemaakt van een aantal bronnen, waaronder concepten van in ontwikkeling zijnde standaarden: [3], [11], [12], en [13].

4.1 Gelaagde bescherming

Good Practice 12
De SCADA-omgeving wordt beveiligd volgens het principe van ‘gelaagde bescherming’ (defence-in-depth).[5]

Achtergrond: De benaderbaarheid van de SCADA-systemen en -netwerken vanuit publieke netwerken en vanuit het bedrijfsnetwerk wordt dusdanig afgeschermd en beveiligd, dat het doorbreken van een beveiliging nog geen ongecontroleerde toegang geeft tot de SCADA-systemen en het SCADA-netwerk. Naast bijvoorbeeld terugbel-systemen, firewalls en eenvoudig controleerbare netwerkkoppelingen kunnen beveiligingsmaatregelen als authenticatie op basis van individuele, regelmatig wijzigende wachtwoorden, indringerdetectie (zie ook [10] punt 7), antivirusmaatregelen en patchbeleid barrières opwerpen voor kwaadwillenden. De kans op ontdekking wordt daardoor vergroot en kans op inbreuk wordt verminderd. Zie ook [10], punt 2.

Status: Een enkel drinkwaterbedrijf heeft geen structurele beveiligingsmaatregelen getroffen. Slechts enkele drinkwaterbedrijven hebben hun beveiliging volgens dit principe ingericht.

4.2 Gescheiden SCADA- en kantoorautomatiseringsomgevingen

Good Practice 13
De SCADA-omgeving is veilig en strikt gescheiden van de kantoorautomatiserings-omgeving (KA).

Good Practice 14
Ingeval van een logische scheiding tussen de kantoorautomatiserings- en de SCADA/ PA-omgevingen met een gedeelde netwerkinfrastructuur gaat de controle over de SCADA-omgeving bewezen niet verloren bij overbelasting van het KA-netwerk.

[5] Zie ook [10], kwetsbaarheid nummer 2.

Achtergrond: Een strikte en vooral eenvoudig gehouden scheiding tussen de kantoorautomatiserings- en de SCADA/PA-omgevingen verhoogt de veiligheid en betrouwbaarheid van de SCADA-omgeving aanzienlijk. SCADA-systemen en SCADA-programmatuur zijn erg gevoelig voor onverwachte door wormen uitgestuurde pakketten en voor netwerkoverbelasting. Dit risico dient daarom ingedamd te worden.
Indien VPNs en concentrators gebruikt worden voor het gelijktijdig gebruik van dezelfde netwerk- en transmissiecomponenten door de KA en de SCADA/PA-omgeving, bestaat het risico dat Trojaanse code of een worm overbelasting veroorzaakt op het (logische) KA-netwerk. Niet alle concentrators en VPN-netwerken geven in een dergelijk geval voldoende capaciteit aan het SCADA-netwerk. Verlies aan monitoring en besturing van SCADA-systemen is dan het gevolg. Daarom is het een goede gewoonte om na iedere netwerkconfiguratiewijziging, die mogelijk van invloed kan zijn op de beschikbaarheid van de SCADA-omgeving, de gevoeligheid van het SCADA-netwerk voor overbelastingen aan de KA-zijde onder gecontroleerde omstandigheden te testen.

Status:. Vijf drinkwaterbedrijven hebben volledig gescheiden netwerken voor SCADA en de KA-omgeving. Eén van die drinkwaterbedrijven gaat over op VPN-technologie.
Eén drinkwaterbedrijf heeft geen enkele scheiding tussen de KA en de PA.
Twee drinkwaterbedrijven passen de VLAN of VPN-technieken toe voor de logische scheiding van de SCADA en administratieve domeinen. Eén van die twee drinkwater-bedrijven gebruikt die VLANs over één fysiek netwerk, de ander mengt alleen de verder fysiek gescheiden netwerken op de verbindingen tussen de verschillende locaties.
Een derde drinkwaterbedrijf plant een overgang naar VPN [1].

4.3 Veilige koppelingen met de SCADA-omgevingen

Good Practice 15
Verwijder alle niet noodzakelijke koppelingen tussen het SCADA-netwerk en andere netwerken.

Good Practice 16
Voer op basis van het vigerende beveiligingsbeleid een sterke, continu bewaakte controle uit op de overgebleven koppeling(en) en de informatie die deze koppeling(en) passeert. (zie ook [8] punten 1 tot en met 3).

Good Practice 17
Ingeval van een noodzakelijke koppeling tussen de SCADA-omgeving en een KA-netwerk, wordt deze bewaakt door een firewall die alleen de noodzakelijke en toegestane diensten doorlaat. De logging van de firewall wordt geregeld gecontroleerd en geanalyseerd op ongeautoriseerd verkeer of pogingen daartoe.

Good Practice 18
De SCADA-omgeving wordt nooit direct gekoppeld met het Internet.

Good Practice 19
De SCADA-omgeving maakt geen gebruik van het Internet als transportdienst, tenzij een aparte risicoanalyse uitgevoerd is m.b.t. denial-of-service (DoS) aanvallen en uitval van de internetinfrastructuur.

Good Practice 20
SCADA-netwerken hebben geen draadloze toegangen (WiFi), tenzij uit een separaat, regelmatig onderhouden expert-risicoanalyseproces blijkt dat het risico beheerst is. Gebruik alle geboden beveiligingsopties (geen zichtbaar baken, hoogste vorm van encryptie, bijvoorbeeld WPA2, MAC-controle). Zie ook [10], punt 5.

Good Practice 21
Modems of andere externe toegangen dienen continu gemonitord te worden en voorzien te zijn van een zwaar authenticatiemechanisme. Autorisaties voor toegang op afstand worden regelmatig gecontroleerd op noodzaak voor continuatie. Uitgangspunt is dat autorisaties alleen verstrekt worden als die noodzakelijk zijn. (zie ook [8] punt 7 en [10] punt 3).

Good Practice 22
De beveiligingsmaatregelen en -instellingen van de netwerkscheidingen (firewalls, routers, VPNs) en koppelingen (modems) worden regelmatig gecontroleerd.

Achtergrond: Ongeautoriseerde beïnvloeding van de SCADA-omgeving wordt, zoveel als mogelijk is, uitgesloten. Koppelingen van de SCADA-omgeving met andere omgevingen zijn kwetsbare plekken. Goede controle over deze koppelingen door het drinkwaterbedrijf is daarom noodzakelijk. Voor interne koppelingen kan een goed geconfigureerde en onderhouden firewall een extra laag ‘defence-in-depth’ bieden. Directe koppelingen met het Internet zijn kwetsbaar voor inbraak en aanvallen op de beschikbaarheid en voor uitval (bijvoorbeeld stroomuitval, kabelproblemen).
Indien Internet en andere publieke netwerken worden gebruikt voor telewerkdiensten, is het aan te bevelen om er een sterke vorm van authenticatie te gebruiken.
Daarnaast is het verstandig om plannen voorhanden te hebben ingeval van storingen in de communicatie-infrastructuur en de elektriciteitvoorziening.

Status: Eén drinkwaterbedrijf gebruikt een gemengde KA-PA omgeving. Eén drinkwaterbedrijf gebruikt Internet als transportdienst. Verschillende drinkwaterbedrijven gebruiken Internet voor telewerktoepassingen met toegang tot de SCADA-omgeving. Driekwart van de drinkwaterbedrijven heeft modemtoegangen tot de SCADA-omgeving welke ook, soms ongecontroleerd, door derden voor onderhoud aan de processystemen en voor storingsassistentie gebruikt worden (zie [1], hoofdstuk 5).
De helft van de drinkwaterbedrijven voert geen regelmatige controle uit op de beveiligingsinstellingen van de netwerkscheidingen en koppelingen.

4.4 Veilige SCADA-systemen en -netwerkcomponenten

Good Practice 23
De SCADA-systemen zijn ’hardened’ en de door de leverancier geboden SCADA-beveiligingsmogelijkheden worden optimaal gebruikt.

Good Practice 24
Het configuratieproces van de SCADA-systemen en -netwerkcomponenten is gedocumenteerd.

Good Practice 25
Het configuratiewijzigingsproces van de SCADA-systemen en -netwerkcomponenten is een gecontroleerd proces.

Good Practice 26
SCADA-systemen zijn - indien mogelijk - voorzien van actuele antivirusprogrammatuur.

Achtergrond: Met hardening van het SCADA-systeem wordt bedoeld dat het systeem dusdanig geconfigureerd wordt dat:
1 Bekende kwetsbaarheden verwijderd zijn.
2 Alle processen die niet essentieel zijn voor de goede werking van het systeem, uit de configuratie verwijderd zijn.
3 Alle poorten en diensten die niet nodig zijn, uitgezet en geblokkeerd zijn.
4 Alle default-toegangen verwijderd zijn.
5 Maak optimaal gebruik van de door leveranciers geboden beveiligingsopties binnen het kader van het eigen SCADA-beveiligingsbeleid.

Het doel van hardening en het gebruik maken van geboden beveiligingsmogelijkheden is om het aantal aangrijpingspunten voor hackers en malware te verminderen (zie ook [8] punten 4 en 6). Goede interne documentatie van de systemen en hun configuraties evenals een configuratiewijzigingsproces verhogen de kans op sneller herstel bij ernstige uitval of het teloorgaan van SCADA-systemen en -netwerken.

Steeds meer SCADA-systemen, ook binnen de drinkwatersector, worden gebaseerd op commercial-off-the-shelf code (Windows, Linux, Open-SCADA, en dergelijke). Daarnaast raken ze gekoppeld aan netwerken die een getrapte verbinding hebben met het Internet of wordt apparatuur van derden gekoppeld aan het SCADA-netwerk. Vroegtijdige detectie van ongewenste code (malware) zoals virussen, wormen en Trojaanse code in de SCADA-omgeving kan helpen het SCADA-netwerk en de systemen vrij te houden van ongewenste malware. Antivirusprogrammatuur is actueel bijgewerkt om zoveel als mogelijk is te voorkomen dat malware een kans krijgt om de leveringszekerheid en kwaliteit van het drinkwater door aantasting van SCADA te verstoren.

Status: Slechts twee drinkwaterbedrijven beveiligen hun SCADA-systemen op deze wijze. Slechts drie drinkwaterbedrijven gebruiken een actuele virusscanner in de SCADA-omgeving.

Good Practice 27
Stel een patchbeleid voor de SCADA-systemen en -netwerkcomponenten vast dat in balans is met het te accepteren bedrijfsrisico van beveiligingsinbreuken door hackers, virussen, Trojaanse code en andere vormen van malware.

Achtergrond: Kwetsbaarheden in systemen raken snel bekend. De cyber criminele wereld bouwt daarna vaak binnen enkele dagen zogenaamde exploits om gevonden kwetsbaarheden uit te buiten. Zodra een patch door de leverancier uitgebracht is, voeren hackers reverse engineering uit om ongepatchte systemen open te breken. SCADA-leveranciers verifiëren patches van bijvoorbeeld Microsoft vaak vrij laat, waardoor SCADA-systemen verhoogd kwetsbaar zijn totdat de patch geverifieerd en vervolgens door het drinkwaterbedrijf geïmplementeerd is. Vooral indien derden systemen (bijvoorbeeld laptops) kunnen aansluiten op het SCADA-netwerk, is het snel doorvoeren van patches een noodzaak om het risico van verstoringen te beheersen.

Status: Twee drinkwaterbedrijven installeren nooit patches. Twee anderen doen dat in principe ook niet, tenzij de leverancier erg sterk aandringt. Een ander bedrijf installeert patches pas na maanden. Een bedrijf patcht slechts éénmaal per jaar.

4.5 Veilige afscherming van de SCADA-omgeving

Good Practice 28
De SCADA-systemen en -netwerken zijn zowel fysiek als elektronisch alleen toegankelijk voor geautoriseerde medewerkers.

Good Practice 29
Alleen vooraf geautoriseerde apparatuur mag gekoppeld worden aan het SCADA-netwerk.

Good Practice 30
Derden sluiten in principe nooit apparatuur (bijvoorbeeld laptops) aan op het SCADA-netwerk en andere bedrijfsnetwerken.
Indien om operationele redenen een uitzondering gemaakt wordt, wordt voorafgaande aan de koppeling zeker gesteld dat de apparatuur/programmatuur volgens de meest actuele definitie virus- en wormvrij is en dat een dergelijke koppeling alleen onder toezicht en verantwoordelijkheid van een medewerker van het drinkwaterbedrijf gemaakt wordt.

Achtergrond: Een derde kan ongewild een virus, worm of Trojaans paard binnenbrengen, dan wel ongeautoriseerde activiteiten ontwikkelen. Laptops en andere apparatuur van derden zijn niet altijd onder stringente beveiligingscontrole. Tevens kan dergelijke apparatuur ongewild toegang tot de SCADA-omgeving geven aan derden indien (per ongeluk) de apparatuur tevens een draadloze netwerkkoppeling toestaat. Opvallend is dat een dergelijk toegang zonder toezicht verleend wordt terwijl men tegelijk stelt wakker te liggen van ongeautoriseerde activiteiten van derden en het risico van door derden binnengebrachte virussen

Status: Twee drinkwaterbedrijven hanteren geen procedures voordat een derde apparatuur mag koppelen met het SCADA-netwerk. Met uitzondering van één drinkwaterbedrijf, mogen derden *zonder toezicht* apparatuur aansluiten op het SCADA-netwerk [1].

4.6 Wachtwoordbeleid voor de SCADA-omgeving

Good Practice 31
Door de leverancier ingestelde standaard gebruiker-wachtwoordcombinaties worden onmiddellijk vervangen door combinaties die door het drinkwaterbedrijf gekozen worden.

Good Practice 32
Wachtwoorden, die toegang geven tot essentiële systeemfuncties, zijn ‘sterk’, zijn alleen op basis van ‘need-to-know’ bekend bij eigen medewerkers en worden regelmatig gewijzigd.

Good Practice 33
Persoonlijke wachtwoorden zijn niet bij anderen bekend en worden regelmatig gewijzigd.

Achtergrond: Om toegang te krijgen tot diensten in het SCADA-netwerk, moet een gebruiker zich eerst authenticeren. Afhankelijk van de gewenste sterkte kan dit enkelvoudig op basis van kennis (gebruikersnaam - wachtwoord combinatie), of meervoudig door extra gebruik van iets dat de gebruiker aantoonbaar bij zich heeft (token) of is (biometrisch kenmerk). Een beveiliging op basis van wachtwoorden alleen wordt als het zwakste gezien. De zwakte van een wachtwoord is mede afhankelijk van de wijze waarop een gebruiker er mee omgaat. De kans dat een wachtwoord door ongeautoriseerden achterhaald wordt is afhankelijk van minimale wachtwoordeisen (lengte, type tekens, niet uit woordenboek, e.d.), de gebruiksfrequentie en de vervangingsfrequentie van het wachtwoord.
De Code voor Informatiebeveiliging [3] stelt in paragraaf 11.2 een aantal beheers-maatregelen op het gebied van wachtwoorden en het wachtwoordbeleid. Daar SCADA-systemen 24 uur, 7 dagen per week gebruikt worden en vaak uit gedistribueerde componenten bestaan, is speciale aandacht voor het wachtwoordgebruik en de daaraan verbonden eisen nodig.

- Het eerste operationele gebod in informatiebeveiliging is dat bij het uitpakken van een nieuw systeem standaardwachtwoorden worden verwijderd dan wel worden gewijzigd. Naast dat de standaard leverancierswachtwoorden veelal simpel te raden zijn, zijn ze ook nog eens publiekelijk gedocumenteerd. Het sleutelkastje tot het systeem en daarmee ook het netwerk staat daarmee wijd open. Zie ook [10] punt 3.
- Gebod twee is dat iedere gebruiker een persoonlijk geheim wachtwoord heeft dat niet met anderen gedeeld wordt. De Code voor Informatiebeveiliging is op dit punt strikt omdat iedere gebruiker daarmee individueel verantwoordelijk gesteld kan worden voor zijn of haar handelingen. Groepsidentificatie is alleen toegestaan wanneer dit ‘geschikt is voor de uit te voeren werkzaamheden’.
- Afhankelijk van de grootte van de organisatie, omloopsnelheid van personeel en aanwezigheid van derden is het een goed gebruik om wachtwoorden met enige regelmaat te wijzigen. In geval van groepsgebonden wachtwoorden is het goed gebruik om zodra een medewerker uit die groep het bedrijf verlaat het wachtwoord te wijzigen.

Status: Twee drinkwaterbedrijven hebben standaard wachtwoorden niet gewijzigd, een derde drinkwaterbedrijf heeft dit deels gedaan. Eén drinkwaterbedrijf gebruikt alleen groepswachtwoorden. Zoals aangegeven in [1] wordt dit als risicovol beschouwd.
Drie drinkwaterbedrijven echter gebruiken alleen persoonlijke wachtwoorden, waarmee in principe volledige toerekenbaarheid geregeld kan worden.

Drie drinkwaterbedrijven geven aan de ooit uitgegeven wachtwoorden nooit te wijzigen. Een ander drinkwaterbedrijf wijzigt de groepswachtwoorden nooit.

Vier drinkwaterbedrijven daarentegen wijzigen de wachtwoorden met een frequentie van tussen de drie maanden en een half jaar en twee van die vier drinkwaterbedrijven wijzigen de groepsgebonden wachtwoorden bij vertrek van een medewerker die toegang heeft tot de SCADA-omgeving.

4.7 Bedrijfscontinuïteit van de SCADA-systemen en -netwerkcomponenten

Good Practice 34
Het bedrijfscontinuïteitbeheer van de SCADA-systemen en -netwerkcomponenten is ingericht conform de Code voor Informatiebeveiliging [3], hoofdstuk 14.
Belangrijk aspect hiervan is dat het drinkwaterbedrijf een goed onderhouden en regelmatig geoefend continuïteitsplan heeft voor de essentiële elementen in de SCADA-omgeving.

Good Practice 35
De essentiële gegevens van SCADA-systemen en -netwerkcomponenten worden op regelmatige basis op een back-up medium opgeslagen (zie ook [8] punt 19).

Good Practice 36
SCADA back-up informatie wordt veilig opgeslagen op een locatie op afstand.

Good Practice 37
Onderdeel van het kwaliteitsproces is het op geregelde tijdstippen nagaan of de back-up informatie bruikbaar is tijdens een hersteloperatie (zie ook [8] punt 19).

Good Practice 38
Het drinkwaterbedrijf heeft een onderhouden en regelmatig geoefend continuïteitsplan voor de essentiële elementen in de SCADA-omgeving (systemen en netwerkcomponenten).

Achtergrond: Calamiteiten in de SCADA-omgeving kunnen zich voordoen, denk aan hardware- en programmatuurstoringen, gevolgen van blikseminslag, brand, water-schade, spanningsproblemen, e.d.. Het snel kunnen inzetten van redundante systemen, reconfigureren en het efficiënt herstel/herladen van SCADA-systemen op een beheerste wijze vergt planvorming vooraf en oefeningen om de leveringszekerheid en de kwaliteit van drinkwater te borgen.

Status: Alle drinkwaterbedrijven hebben hun configuratiegegevens ook elders ondergebracht. Het merendeel van de bedrijven heeft redundantie in hun configuraties en gedistribueerde controlecentra. Vier drinkwaterbedrijven geven aan geen geteste uitwijkplannen te hebben. Eén van die bedrijven heeft meer decentrale configuraties en geeft aan het risico daarmee in te dekken. Drie drinkwaterbedrijven hebben geen calamiteitenafspraken met hun toeleveranciers.

4.8 Beheer van informatiedragers in de SCADA-omgeving

Good Practice 39
Informatiedragers uit de SCADA-omgeving worden op adequate wijze beheerd en op gecontroleerde wijze buiten gebruik gesteld.

Achtergrond: Op informatiedragers die in gebruik zijn in de SCADA-omgeving kan bedrijfsgevoelige informatie als configuratiegegevens staan. Bij buitengebruikstelling van de gegevensdrager of de apparatuur waarin deze is ingebouwd (ingebouwde harde schijven) is het verstandig dat de informatie op afdoende wijze gewist wordt of dat de informatiedrager vernietigd wordt.

5 Achtergrondliteratuur

5.1 Management van Informatiebeveiliging

- Ir. H.A.M. Luiijf en Ir. R. Lassche,
  SCADA (on)veiligheid: een rol voor de overheid?,
  TNO-KEMA rapport, april 2006.
- ISO, Information technology - Security techniques - *Code of practice for information security management framework*, ISO/IEC 17799:2005.

  Naar verwachting wordt de Code in de loop van 2007 hernummerd tot ISO/IEC 27002:2007. De Nederlandse versie De Nederlandse 'Code voor Informatiebeveiliging' is verschenen als NEN-ISO/IEC 17799:2005.en is te bestellen bij het NEN te Delft. De internationale versie is via www.iso.ch verkijgbaar.
- ISO, Information technology -- Security techniques -- *Information security management systems -- Requirements,* ISO/IEC 27001:2005.

  Het bij ISO/IEC 17799:2005 behorende, certificeerbare management framework.
- G. Finco, et al.,
  Cyber Procurement Language for Control Systems version 1.6,
  INL Critical Infrastructure Protection/Resilience Center, Idaho Falls,
  June 2006. On-line:
  http://www.msisac.org/scada/documents/12July07_SCADA_procurement.pdf

5.2 Bewustwording

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

5.3 Informatiebeveiliging en SCADA/procescontrole

- E.M.M. Castelijn, J.G.J. Nijhuis, *Informatiebeveiliging Waterbedrijven*,
  VEWIN Augustus 2004.
- N. Lammers, N.T.C. Zantkuyl, Update *Informatiebeveiliging Waterbedrijven*,
  VEWIN, maart 2007.
  De bovenstaande twee publicaties tezamen geven de drinkwatersector handvatten voor de brede aanpak van informatiebeveiliging in de sector op basis van de ISO/IEC 17799:2005 standaard (Code voor Informatiebeveiliging). Deze good practices geven op basis van de eerdere analyse handvatten om de procesautomatiserings-/SCADA-specifieke problematiek aan te pakken.
- 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

  Dit (concept)rapport beschrijft deels dezelfde onderwerpen als de TNO/KEMA studie en gaat in op een aantal SCADA-zwakheden. Hoofdstuk 5 geeft achtergrondinformatie voor juiste firewall instellingen op de grens tussen de PA- en de KA-omgevingen. Hoofdstuk 6 geeft een SCADA-

specifieke invulling van ‘controls’ zoals die te vinden zijn in de Code voor Informatiebeveiliging. Het rapport bevat een uitgebreide lijst met literatuur- en webreferenties.

- ISA, *ISA-TR99.00.01-2007 -- Security Technologies for Industrial Automation and Control Systems, Instrumentation, Systems, and Automation Society*, (draft) Technical Report 2007.

  Dit (concept)rapport bevat de beschrijving van technische SCADA-beveiligingsonderwerpen als authenticatie en autorisatietechniek, firewalls en versleuteling, indringerdetectietechniek; bekende zwakheden en aanbevelingen voor de aanpak van die zwakheden. Het is gedetailleerder dan het hierboven genoemde NIST SP800-82. Het rapport bevat een uitgebreide lijst met literatuur- en webreferenties.

5.4 SCADA-netwerkbeveiliging

- NISCC, *Good Practice Guide on Firewall Deployment for SCADA and Proces Control Networks*, 2005.
  Zie website: http://www.cpni.gov.uk/ ga naar *Products and Services* en ga vervolgens naar Good Practices. Selecteer daar 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
- Luiijf, H.A.M., *Slachtoffer van computercriminaliteit, wat dan?*, Beveiliging, november 2007.
- ECP.NL/KWINT programma, *Voorlichtingsmateriaal (potentiële) computercriminelen*, 2005. On-line: http://www.ecp.nl/download/ Voorlichtingsmateriaal_tbv_(potentiële)_computercriminelen.pdf
- GovCert.NL, *Van herkenning tot Aangifte*, Den Haag, 2005.
  On-line: http://www.govcert.nl/render.html?it=39

5.5 Webverzamelingen SCADA

- http://www.cpni.gov.uk
  Verzameling van voornamelijk op het management gerichte SCADA Good Practice Guides, zie de website:van het VK Centre for the Protection of National Infrastructure, (klik Products and Services, klik Good Practices).
- http://www.us-cert.gov/control_systems/index.html
  Veel documenten en referenties over SCADA-beveiliging.
- http://csrc.nist.gov/publications/
  Veel good practices op deelgebieden van informatiebeveiliging van systemen en netwerken, waaronder SCADA, firewalls, informatiemediabeheer en dergelijke.
- http://www.thei3p.org/site_index/
  Veel recente Amerikaanse research- en good practicedocumenten op SCADA-gebied van het Institute for Information Infrastructure Protection (I3P).
- http://www.scadasec.net/secwiki/ScadaSec
  Links naar verschillende SCADA-papers, standaardisatiegroepen en andere interessante SCADA-bronnen.

5.6 Amerikaanse bronnen voor de watersector

- http://www.waterisac.org
  Links naar een aantal drinkwaterorganisaties, literatuur en achtergrondinformatie.

6 Referenties

[1] Ir. H.A.M. Luiijf,
Analyse SCADA-veiligheid in de Nederlandse drinkwatersector,
rapport TNO-DV 2007 C317, juli 2007. rubricering: NICC Vertrouwelijk

[2] Ir. H.A.M. Luiijf en Ir. R. Lassche,
SCADA (on)veiligheid: een rol voor de overheid?, TNO-KEMA rapport, april 2006.

[3] ISO, Code voor Informatiebeveiliging/*Information technology - Security techniques - Code of practice for information security management framework*, ISO/IEC 17799:2005
Noot: wordt eerdaags omgenummerd in ISO/IEC 27002; de Nederlandse versie is verschenen als 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.

[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.

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

7 Ondertekening

Den Haag, december 2007

ir. R.F.W.M. Willems
Afdelingshoofd

TNO Defensie en Veiligheid

ir. H.A.M. Luiijf
Auteur

A Checklists Good Practices

Tabel A 1 SCADA Good Practices voor het managementteam

Hoofdonderwerp	**Good Practice**	√
Bedrijfsbeveiligingsbeleid	#1 Algemeen informatiebeveiligingsbeleid met gekoppeld specifiek SCADA-beveiligingsbeleid #2 Code voor Informatiebeveiliging en beveiligings-managementsysteem #3 SCADA-specifiek beleid is verlengde van algemeen beveiligingsbeleid #4 SCADA-informatiebeveiligingsbeleid omvat fysieke beveiliging #5 Vastgelegde taken, verantwoordelijkheden en bevoegdheden	
Risicomanagement	#6 SCADA is onderdeel van bedrijfsrisicomanagement	
Beveiligingsbewustwording	#7 Doorlopend beveiligingsbewustzijnsprogramma	
Audit	#8 Er is minimaal jaarlijks een EDP audit van de SCADA omgeving	
Verwervingsbeleid	#9 Calamiteitenparagraaf bij verwerving/contracten #10 Beveiligingseisen onderdeel van verwerving #11 Beveiligingsparagraaf in contracten voor onderhoud /werkzaamheden derden	

Tabel A 2 SCADA Good Practices voor het technisch PA-managementteam

Hoofdonderwerp	**Good Practice**	√
Gelaagde bescherming	#12 Principe van 'gelaagde bescherming' (defence-in-depth)	
Gescheiden SCADA- en KA-omgevingen	#13 SCADA-omgeving veilig en strikt gescheiden van KA #14 Gegarandeerde beschikbaarheid gedeeld netwerk	
Veilige koppelingen met de SCADA-omgevingen	#15 Verwijder niet noodzakelijke koppelingen #16 Continu bewaakte controle op koppelingen #17 Strikt geconfigureerde en bewaakte firewalls #18 Geen directe Internetkoppeling met de PA-omgeving #19 Geen gebruik van Internet als transportdienst #20 Geen draadloze toegangen tot de SCADA-omgeving #21 Strikt regime inbelmodems/externe toegang #22 beveiligingsmaatregelen en -instellingen netwerk-scheidingen en koppelingen worden regelmatig gecontroleerd	
Veilige SCADA-systemen en -netwerkcomponenten	#23 Hardened/optimaal beveiligde systemen #24 Gedocumenteerde configuraties #25 Beheerst configuratiewijzigingsproces #26 Actuele antivirusprogrammatuur #27 Adequaat patchbeleid	
Veilige afscherming van de SCADA-omgeving	#28 Fysieke en elektronische afscherming SCADA-systemen en netwerkcomponenten #29 Alleen geautoriseerde apparatuur koppelen aan SCADA-netwerk #30 Apparatuur derden wordt niet gekoppeld, tenzij ..	
Wachtwoordbeleid voor de SCADA-omgeving	#31 Standaardwachtwoorden onverwijld vervangen #32 Essentiële wachtwoorden: sterk, beperkte kring, regelmatig vervangen #33 Persoonlijke wachtwoorden: strikt persoonlijk; regelmatig vervangen	
Bedrijfscontinuïteit SCADA	#34 Conform Code voor Informatiebeveiliging [3] H14 #35 Regelmatige back-up van SCADA-systemen #36 Veilige opslag back-ups #37 Regelmatige controle bruikbaarheid/volledigheid back-up #38 Onderhouden en geoefend continuïteitsplan	
Beheer van SCADA informatiedragers	#39 Adequaat beheer; gecontroleerde afvoer	

Distributielijst

2 ex.	Brabant Water
2 ex.	Duinwaterbedrijf Zuid-Holland
2 ex.	PWN Waterleidingbedrijf Noord-Holland
2 ex.	Vitens
2 ex.	Waterleidingmaatschappij Drenthe
2 ex.	Waterleidingmaatschappij Groningen
2 ex.	Waterleidingmaatschappij Limburg
2 ex.	Waternet
2 ex.	NICC t.b.v. Evides (zodra aangesloten)
2 ex.	NICC t.b.v. Oasen (zodra aangesloten)
5 ex.	NICC intern exemplaar
2 ex.	TNO Defensie en Veiligheid, locatie Den Haag dr. M.H.A. Klaver ir. H.A.M. Luiijf
1 ex.	TNO Defensie en Veiligheid, locatie Den Haag Archief