TASKFORCE
Bestuur & Informatieveiligheid Dienstverlening

# ICS/SCADA

Een operationeel product op basis van de informatiebeveiligingsbaselines voor waterschappen (BIWA), het Rijk (BIR), provincies (IBI) en gemeenten (BIG)

Rijksoverheid VNG Vereniging van Nederlandse Gemeenten Interprovinciaal Overleg ip MANIFESTgroep UNIE VAN WATERSCHAPPEN

## Colofon

Onderhavig operationeel product, behorende bij de Baseline Informatiebeveiliging Waterschappen (BIWA), Baseline Informatiebeveiliging Rijksdienst (BIR), Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en de Interprovinciale Baseline Informatiebeveiliging (IBI) is mogelijk gemaakt door de Taskforce Bestuur en Informatieveiligheid Dienstverlening (Taskforce BID).

## Leeswijzer

Dit document is een operationeel product op basis van de informatiebeveiligingsbaselines voor waterschappen (BIWA), het Rijk (BIR), provincies (IBI) en gemeenten (BIG).

### Doel

Dit document biedt een handreiking ten aanzien van informatiebeveiliging voor het gebruik van ICS/SCADA door waterschappen, Rijksoverheidsorganisaties, provincies en gemeenten. De uitgangspunten over informatiebeveiliging voor het gebruik van ICS/SCADA zijn afkomstig uit de informatiebeveiligingsbaselines BIWA, BIR, IBI en de BIG. Verschillen tussen baselines die relevant zijn voor het gebruik van ICS/SCADA of verschillen in specifieke handreikingen voor (een) bepaalde doelgroep(en) worden aangegeven.

### Doelgroep

Dit document is bedoeld voor beheerders van ICS/SCADA-systemen, de informatiebeveiligingsorganisatie onder leiding van de CISO en het verantwoordelijke management van de organisatie.

### Reikwijdte

Het document gaat in op personele, organisatorische en technische aspecten die organisaties dienen te overwegen in relatie tot informatiebeveiliging van ICS/SCADA.

### Relatie met overige producten

- Baseline Informatiebeveiliging Waterschappen (BIWA)
- Baseline Informatiebeveiliging Rijksdienst (BIR)
- Interprovinciale Baseline Informatiebeveiliging (IBI)
- Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)
- Voorschrift Informatiebeveiliging Rijksdienst (VIR:2007)
- Informatiebeveiligingsbeleid

## Inhoudsopgave

# 1 Inleiding

## 1.1 Aanleiding

Het vierde Cybersecuritybeeld Nederland[1] van het Nationaal Cyber Security Center (NCSC) stelt dat verbetering van de beveiliging van ICS/SCADA-systemen (Industrial Control Systems/Supervisory Control And Data Acquisition) aandacht blijft verdienen. 'Het belang van dergelijke systemen voor de vitale processen in de samenleving staat buiten kijf'[2]. Het aantal kwetsbaarheden blijft toenemen, net als de connectiviteit van oude (legacy) systemen. Ondanks de beperkte beveiliging van veel ICS/SCADA worden ze wel steeds vaker op afstand vanuit een centraal punt bestuurd. Dit verhoogt het risico op veiligheidsincidenten, omdat er mogelijk via internet toegang kan worden verkregen tot systemen. Doordat oude(re) systemen of *embedded devices*[3] niet zijn gebouwd volgens het principe van *security by design*, waarmee wordt bedoeld dat beveiliging niet als kernbestanddeel in het ontwerp is meegenomen, is het beveiligen tegen huidige dreigingen niet eenvoudig. Veel (lokale) overheidsorganisaties maken gebruik van ICS/SCADA voor belangrijke processen, zoals het bedienen van bruggen en sluizen, het aansturen van gemalen voor oppervlakte water, het aansturen van verkeerslichten, camerasystemen of drinkwater- en afvalwaterinstallaties.

In dit document wordt een handreiking geboden om de beveiliging te verbeteren van ICS/SCADA door waterschappen, Rijksoverheidsorganisaties, provincies en gemeenten. In dit document ligt de nadruk op het verhogen van de bewustwording op het onderwerp, het verkrijgen van inzicht in en controle op de beveiligingsrisico's, het bieden van 'quick wins' en structurele aandachtspunten voor de beveiliging.

Voor het afleiden van beveiligingseisen ten aanzien van ICS/SCADA wordt gebruikt gemaakt van de uitgangspunten en de beveiligingseisen uit de informatiebeveiligingsbaselines voor de waterschappen (BIWA), het Rijk (BIR), provincies (IBI) en gemeenten (BIG).[4]

## 1.2 ICS/SCADA

ICS/SCADA (Industrial Control Systems/Supervisory Control And Data Acquisition) zijn meet- en regelsystemen die worden gebruikt voor de aansturing van industriële processen of gebouwbeheersystemen. ICS is de algemene term voor procesbesturing. Met SCADA wordt alleen de overkoepelende procesbesturing ten behoeve van het verzamelen en analyseren van real-time procesinformatie bedoeld,[5] die gebruikt wordt om systemen over grote geografische afstanden aan te sturen, zoals die bij waterzuivering of energievoorziening voor komen. SCADA-systemen verzamelen en verwerken meet- en regelsignalen van sensoren in fysieke systemen en regelen de aansturing van de bijbehorende machines of apparaten. In tegenstelling tot het begrip *Industrial Control Systems (ICS)*, wordt veelal onterecht het

[1] NCSC (2014).
[2] Idem, p. 43.
[3] Embedded devices zijn systemen waarbij de software in een chip is geïntegreerd. Deze 'embedded software' is niet of nauwelijks te wijzigen zonder vervanging.
[4] BIWA, Baseline Informatiebeveiliging Waterschappen; BIR, Baseline Informatiebeveiliging Rijksdienst; IBI, Interprovinciale Baseline Informatiebeveiliging; en BIG, Baseline Informatiebeveiliging Nederlandse Gemeenten.
[5] NCSC (2012a).

begrip *SCADA* gebruikt om alle systemen te beschrijven die fysieke processen besturen. Deze brede interpretatie van het begrip SCADA kan met name bij specialisten tot verwarring leiden. SCADA is een groep van systemen die valt onder de brede noemer van Industrial Control Systems.

In dit document worden de begrippen pragmatisch ingevuld, waarbij wordt geaccepteerd dat het begrip SCADA door niet-specialisten wordt gebruikt om alle ICS te benoemen. Hier worden de begrippen breed geïnterpreteerd en daarom gesproken over ICS/SCADA en worden ook beveiligingsissues voor gebouwbeheersystemen, camerasystemen (CCTV), toegangscontrole, klimaatcontrole (HVAC), slimme-energiemeters meegenomen.[6]

## 1.3 Doelstelling en scope

Dit document heeft tot doel een praktische handreiking te bieden voor het verhogen van het basisniveau van de beveiliging van ICS/SCADA door waterschappen, Rijksoverheidsorganisaties, provincies en gemeenten. Het doel is om de beveiliging van ICS/SCADA op orde te krijgen en onder controle te houden. Net als de baselines richt dit document zich zowel op de menselijke, organisatorische als technische aspecten van de beveiliging van ICS/SCADA. Indien nodig worden doelgroepspecifieke aandachtspunten apart toegelicht.

Er wordt veel gepubliceerd op dit thema, waarvan voor het opstellen van dit document gebruik is gemaakt. In dit document wordt geen volledige (technische) achtergrond en context beschreven ten aanzien van ICS/SCADA en de beveiliging van deze systemen. Het document is tot stand gekomen na documentenstudie en interviews met experts.

## 1.4 Leeswijzer

In hoofdstuk 2 wordt beknopt beschreven wat ICS/SCADA is. Ingegaan wordt op de toepassingsgebieden, de relatie met reguliere IT-systemen, ontwikkelingen ten aanzien van ICS/SCADA en de organisatorische inrichting van het beheer en verantwoordelijkheden voor ICS/SCADA. In hoofdstuk 3 worden de beveiligingsaspecten van ICS/SCADA voor organisaties toegelicht, waarbij aandacht is voor risico's en aandachtspunten voor de beveiliging. In hoofdstuk 4 wordt een concrete handreiking geboden voor het op orde en onder controle krijgen van de beveiliging van ICS/SCADA. Om dit bereiken zijn daarvoor in hoofdstuk 4 drie stappen onderscheiden: (1) Inzicht, (2) Quick wins en (3) Structureel verbeteren. In bijlage 1 wordt een voorbeeld voor een ICS/SCADA-beleidsdocument gepresenteerd.

[6] Byres (2012).

# 2 ICS/SCADA

## 2.1 Inleiding

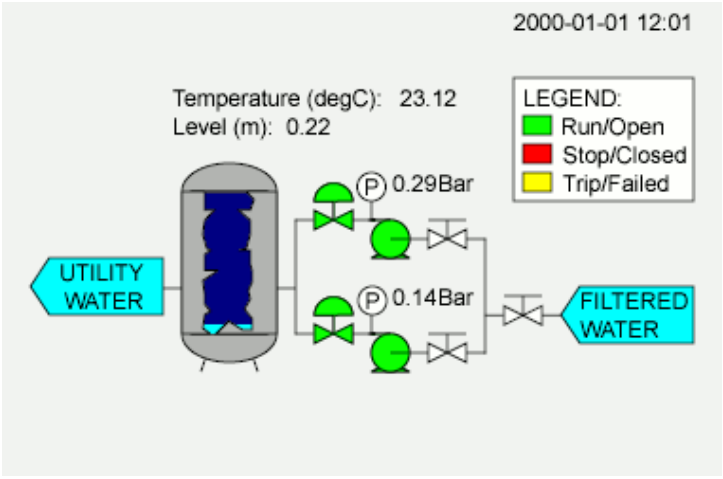
In dit hoofdstuk wordt de achtergrond en context bij ICS/SCADA beschreven. Paragraaf 2.2 gaat in op de definitie van ICS/SCADA, de toepassingsgebieden, de verhouding tot reguliere IT-systemen en de ontwikkeling van ICS/SCADA in relatie tot 'Internet of Things'. In paragraaf 2.3 wordt de inrichting van ICS/SCADA in overheidsorganisaties toegelicht.

## 2.2 ICS/SCADA

### Wat is ICS/SCADA?

ICS/SCADA (Industrial Control Systems/Supervisory Control And Data Acquisition)-systemen zijn meet- en regelsystemen. Industrial Control Systems (ICS) is de algemene term om procesbesturingssystemen te beschrijven, waar SCADA-systemen een specifiek deel van zijn. SCADA-systemen verzamelen en verwerken meet- en regelsignalen van sensoren in fysieke systemen en regelen de aansturing van de bijbehorende machines of apparaten. SCADA is de overkoepelende procesbesturing op een systeem ten behoeve van het verzamelen en analyseren van real-time procesinformatie, die gebruikt wordt om systemen vaak over grote geografische afstanden aan te sturen, zoals die bij gasleidingen, waterzuivering of de energievoorziening voor komen.

ICS/SCADA bieden de mogelijkheid tot het visualiseren van fysieke procesgegevens, het aansturen van processen en automatische alarmering.[7] ICS/SCADA worden in een veelheid van toepassingen en organisaties gebruikt. Als meet- en regelsystemen de bedrijfsvoering ondersteunen dan zijn ICS/SCADA nagenoeg onmisbaar. Het op afstand besturen van processystemen is effectiever en efficiënter dan fysiek ter plaatse gaan en systemen te bedienen. Onder andere Siemens, General Electric, ABB en Schneider Electric zijn bekende leveranciers van ICS/SCADA.




*Voorbeeld van een SCADA-systeem*[8]

[7] NOREA (2014).
[8] Wikipedia (2014b).

### Toepassingsgebieden

ICS/SCADA worden voor een veelheid aan toepassingen ingezet. Bij waterschappen, gemeenten, provincies en Rijksoverheidsorganisaties zijn ICS/SCADA voornamelijk terug te vinden in de volgende gebieden:

| Toepassing | Organisatie |
|---|---|
| Bruggen, sluizen, gemalen, stormvloedkeringen | Waterschappen, gemeenten, provincies, Rijksoverheidsorganisaties |
| Afvalwaterinstallaties | Waterschappen, gemeenten |
| Drinkwaterinstallaties | Drinkwaterbedrijven (eigendom van provincies en/of gemeenten) |
| Verkeersregeling, (verkeerslichten, tunnels) | Gemeenten, provincies, Rijksoverheidsorganisaties |
| Gebouwbeheersing (klimaatbeheersing, brandmelding, roltrappen, liften) | Waterschappen, gemeenten, provincies, Rijksoverheidsorganisaties |
| Sensoren (camera systemen, verkeerstellers, detectielussen) | Waterschappen, gemeenten, provincies, Rijksoverheidsorganisaties |
| Toegangsbeveiliging (slagbomen, elektronische hekwerken) | Waterschappen, gemeenten, provincies, Rijksoverheidsorganisaties |
| Parkeergarages | Waterschappen, gemeenten, provincies, Rijksoverheidsorganisaties |
| Zwembaden | Gemeenten |

### ICS/SCADA en reguliere IT

ICS/SCADA en reguliere IT-systemen (zoals kantoorautomatisering, netwerken, internet) groeien steeds meer naar elkaar toe. Doordat ICS/SCADA steeds meer op IT gaat lijken en direct of indirect (via het bedrijfsnetwerk of door bediening op afstand) op het internet wordt aangesloten, staan ICS/SCADA ook steeds meer bloot aan dezelfde dreigingen als IT.[9]

[9] ENISA (2013a), p.1.

Tussen veel ICS/SCADA en IT-systemen blijven tegelijkertijd kenmerkende verschillen bestaan die ook van invloed zijn op de beveiliging. Standaard IT-beveiligingsoplossingen kunnen niet één op één worden overgenomen in een ICS/SCADA omgeving. Patch management moet ook worden ingericht voor ICS/SCADA, maar volgens een andere werkwijze dan bij reguliere IT. Hetzelfde geldt voor het inrichten van toegangsbeveiliging, firewalls, de architectuur, en alle andere aspecten van ICS/SCADA. IT-oplossingen moeten in veel gevallen toepasbaar worden gemaakt voor het specifieke gebruik en de techniek van ICS/SCADA.

Het aansturen van fysieke processen door ICS/SCADA stelt onder meer andere eisen aan prestaties, beschikbaarheid en architectuur. Het uitvallen van de aansturing, fouten en andere verstoringen van fysieke processen is zeer onwenselijk. Dit kan hoge (productie)kosten veroorzaken door schade aan systemen en verstoring van continuïteit van bedrijfsprocessen. De operatie van ICS/SCADA is daarnaast meestal 24 uur per dag, 7 dagen per week, waar voor IT-systemen de nadruk ligt op kantoortijden. De mogelijkheden om beheer en onderhoud te plegen op ICS/SCADA is daardoor heel beperkt. Patch management dient stringenter gepland te worden en patches moeten uitgebreider worden getest voordat het in productie kan worden genomen, omdat de potentiële schade veel groter is.[10]

Een onderscheid in levensduur tussen ISC/SCADA en IT-systemen, van 15 tot 20 jaar voor ICS/SCADA tot drie tot vijf jaar voor IT, betekent dat het beheer, onderhoud en integratie van ICS/SCADA wordt bemoeilijkt op dezelfde manier als bij IT-legacy systemen. Het toepassen van specifieke hard- en software voor ICS/SCADA en vaak eigen besturingssystemen en protocollen van leveranciers draagt daar tevens aan bij. ISC/SCADA kan tevens bestaan uit zogenaamde embedded software die niet of nauwelijks te wijzigen kan zijn zonder vervanging.

Op dit moment worden steeds vaker bekende IT-oplossingen toegepast om de systemen te uniformeren, te automatiseren, de connectiviteit te vergroten en onderling te integreren. Deze trends veroorzaken grote sprongen in effectiviteit en efficiëntie, maar brengt nieuwe beveiligingsrisico's met zich mee.

De toegenomen connectiviteit maakt tevens nieuwe bedrijfsmodellen mogelijk voor organisaties. Vergelijkbaar met IT-systemen wordt het beheer voor ICS/SCADA steeds meer uitbesteed aan derde partijen.

### ICS/SCADA als Internet of Things

De ontwikkelen ten aanzien van ICS/SCADA worden in één adem genoemd met de trend van 'Internet of Things' (IoT), dat het aansluiten van fysieke voorwerpen met het internet beschrijft. Fysieke apparaten worden vaker zelfstandig opererende objecten met de potentie tot het nemen van autonome beslissingen en autonome communicatie met andere objecten

[10] ENISA (2013b).

en personen op het internet.[11] Voor consumenten biedt Internet of Things de mogelijkheid om bijvoorbeeld centraal en op afstand huishoudelijke apparatuur als de verwarming of de vaatwasser te besturen. Dit kan het gebruik vergemakkelijken en energievoordelen opleveren. Voor organisaties betekent het centraal en (deels) geautomatiseerd aansturen van fysieke processen, zoals sluizen of verkeerslichten, efficiëntere processen voor beheer en integratie met andere systemen, en minder kosten voor infrastructuur. Als procesinformatie van verschillende systemen bij elkaar wordt gebracht, biedt dit ook gelegenheid voor procesverbetering.

## 2.3 ICS/SCADA in organisaties

De veelheid aan toepassingsgebieden van ICS/SCADA draagt bij aan een zeer decentrale inrichting van het gebruik en beheer in organisaties. Bij waterschappen, gemeenten, provincies en Rijksoverheidsorganisaties is er doorgaans sprake van één ondersteunende IT-organisatie, maar er bestaat geen centrale organisatie voor ICS/SCADA. Het organisatieonderdeel dat voor zijn taken en verantwoordelijkheden gebruik maakt van ICS/SCADA is in veel gevallen ook verantwoordelijk voor het beheer en onderhoud van ICS/SCADA. Dit geldt ook voor de ICS/SCADA toegepast in gebouwen en objecten (zoals zwembaden, bruggen). Het facilitair management van de locatie is meestal verantwoordelijk voor het goed functioneren van de systemen op die locatie.

| Waterschappen | Gemeenten | Provincies | Rijksoverheid |
|---|---|---|---|
| Huisvesting/facilitair | Huisvesting/facilitair | Huisvesting/facilitair | Huisvesting/facilitair |
| IT | IT | IT | IT |
| Inkoop | Inkoop | Inkoop | Inkoop |
| Waterbeheer | Wonen | | Wonen |
| Zuiveringsbeheer | Verkeer/infrastructuur | Verkeer/infrastructuur | Verkeer/infrastructuur |
| Waterkeringsbeheer | | | |

*Inrichting van ICS/SCADA in organisaties.*

Ondanks de veelal decentrale inrichting van de ICS/SCADA-organisatie is het lijnmanagement (de directie) verantwoordelijk voor het veilig gebruik van ICS/SCADA.

Bij een aantal organisaties, waaronder waterschappen, is onder meer omwille van de veiligheid van systemen de ICS/SCADA zo volledig als mogelijk gescheiden van de reguliere IT-organisatie. Een scheiding tussen de ICS/SCADA en de IT vermindert het dreigingsoppervlak voor de ICS/SCADA en de kans op aanvallen via de IT. Kosten voor infrastructuur en beheer lijken wel toe te nemen.

[11] Wikipedia (2014a).

# 3 Beveiliging van ICS/SCADA

## 3.1 Inleiding

In dit hoofdstuk wordt de beveiliging van ICS/SCADA beschreven. In paragraaf 3.2 wordt ingegaan op de risico's van ICS/SCADA voor (lokale) overheidsorganisaties. In paragraaf 3.3 wordt gekeken naar de kwaliteitsaspecten die voor de beveiliging van ICS/SCADA belangrijk zijn. In paragraaf 3.4 worden algemene aandachtspunten behandeld voor het beveiligen van ICS/SCADA verdeeld in de categorieën mensen *(people)*, processen *(process)* en technologie *(technology).*

## 3.2 Risico's van ICS/SCADA voor uw organisatie

Niet- of slecht-beveiligde ICS/SCADA kan verschillende risico's voor organisaties hebben. De gevolgen van het ontbreken van een juiste digitale beveiliging ('security') bij ICS/SCADA kan leiden tot fysieke veiligheidsproblemen ('safety') voor mensen, de omgeving, apparatuur en installaties. Onbevoegden kunnen toegang krijgen tot (proces)informatie en tot de besturing van processen. Afhankelijk van de mate van beveiliging, kunnen delen van het proces worden gemanipuleerd.[12,13] Het is in bepaalde gevallen niet eens nodig om specifiek kennis te hebben om processen te manipuleren. Tegelijkertijd blijkt dat de gemotiveerde, vaardige aanvaller, de zogenaamde Advanced Persitent Threat (APT), steeds vaker geïnteresseerd is in ICS/SCADA.[14] De potentiële gevolgen zijn afhankelijk van de aard van het proces. Voor reputatieschade door negatieve publiciteit is het eenvoudige gegeven van het falen van beveiliging vaak minstens zo belangrijk als de feitelijke gevolgen van een aanval. Het vertrouwen van burgers in overheidsorganisaties brengt een hoge verantwoordelijkheid met zich mee ten aanzien van de kwaliteit en de veiligheid die organisaties moeten bieden.

Het risico neemt de afgelopen jaren toe door de beschikbaarheid van gratis online zoekmachines en hackingtools waardoor het zelfs voor niet ICS/SCADA-specialisten steeds makkelijker wordt om (eenvoudige) aanvallen uit te voeren of om informatie te verzamelen voor een complexe aanval.[15]

*Oorzaken van onvoldoende beveiliging*

De voornaamste beveiligingsrisico's ten aanzien van ICS/SCADA ontstaan volgens onderzoekers door vier oorzaken:[16]

- Het gebrek aan zorgen over beveiliging en authenticatie in het ontwerp, de implementatie en werking van bepaalde ICS/SCADA netwerken;

[12] NCSC (2012a), p.2.
[13] Idem, p.1.
[14] Idem.
[15] Voorbeelden van gratis online tools zijn SHODAN, NMAP, Nessus, Metasploit. Ook systeemeigenaren kunnen deze tools gebruiken om zelf te onderzoeken of er systemen van hun organisatie online te vinden zijn en of die systemen mogelijk kwetsbaar zijn.
[16] Wikipedia (2014b).

- Het geloof dat ICS/SCADA het voordeel van ‘security through obscurity’ (het geheim houden van beveiligingsmaatregelen) hebben door het gebruik van gespecialiseerde protocollen en producten van leveranciers;
- Het geloof dat ICS/SCADA netwerken veilig zijn, omdat ze fysiek beveiligd zijn;
- Het geloof dat ICS/SCADA netwerken veilig zijn, omdat ze niet met internet verbonden zijn.

## 3.3 Beveiliging voor ICS/SCADA

Voor de beveiliging van informatiesystemen wordt gekeken naar de volgende drie kwaliteitsaspecten om de informatiebeveiliging te garanderen:

- *Beschikbaarheid (B):* het zorg dragen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers;
- *Integriteit (I):* het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking;
- *Vertrouwelijkheid (V)*: het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn.

De baselines voor informatiebeveiliging voor waterschappen (BIWA), gemeenten (BIG), provincies (IBI) en Rijksoverheidsorganisaties (BIR) zijn, net als de richtlijnen van de ISO voor informatiebeveiliging, gebaseerd op deze BIV-aspecten van informatiebeveiliging.

*Voor ICS/SCADA prioriteit bij integriteit en beschikbaarheid*

Voor ICS/SCADA is de integriteit van de systemen het belangrijkst. Integriteit betreft de juistheid van de output van sensoren en metingen, waarop de sturing van processen wordt gebaseerd. Als die begindata niet overeenkomt met de werkelijkheid, dan kunnen fysieke verstoringen in het proces worden veroorzaakt. De beschikbaarheid van ICS/SCADA is tevens essentieel voor het kunnen uitvoeren van belangrijke bedrijfsprocessen. Het niet beschikbaar zijn van processen (zoals het sluiten van sluizen of het aansturen van gemalen) kan leiden tot fysieke schade of veiligheidsrisico’s. Verstoringen, door bijvoorbeeld patch management, moeten derhalve ruim van tevoren worden ingepland. De vertrouwelijkheid van gegevens is minder van belang. Reguliere IT-systemen verwerken veel vertrouwelijke overheidsinformatie, bedrijfsgegevens of persoonsgegevens. De vertrouwelijkheid en de integriteit van de gegevens is voor IT-systemen het belangrijkst.

| Belang van het kwaliteitsaspect | ICS/SCADA | Reguliere IT |
|---|---|---|
| 1 | Integriteit | Vertrouwelijkheid |
| 2 | Beschikbaarheid | Integriteit |
| 3 | Vertrouwelijkheid | Beschikbaarheid |

*Het verschil in het belang van kwaliteitsaspecten voor ICS/SCADA en reguliere IT.*

*ICS/SCADA beveiligen betekent IT-beveiligingsoplossingen herinrichten*

Voor het beveiligen van ICS/SCADA is het belangrijk de verschillen met reguliere IT in ogenschouw te houden, maar zeker ook de overeenkomsten. Beveiliging van ICS/SCADA hoeft niet opnieuw te worden uitgevonden. Innovatie van IT-beveiligingsoplossingen door deze toepasbaar te maken en aanvullend in te zetten voor ICS/SCADA levert veel beveiligingswinst op. Net als bij IT moeten voor ICS/SCADA risico analyses, GAP-analyses, bewustwording, training en sturing, patch management, toegangsbeveiliging, beveiliging in de architecture (*security by design*), beheer en netwerkbeveiliging (encryptie, firewalls) worden uitgevoerd en ingericht.

## 3.4 Aandachtspunten voor beveiliging

In deze paragraaf worden algemene aandachtspunten voor het beveiligen van ICS/SCADA besproken. In hoofdstuk 4 worden Quick wins beschreven. De aandachtspunten zijn verdeeld in de categorieën mensen *(people)*, processen *(process)* en technologie *(technology)*.

**Mensen**

Voor het juist beveiligen van ICS/SCADA dienen verantwoordelijken bewust te zijn van de risico's, voldoende expertise te hebben, en tijd en middelen te krijgen voor het uitvoeren van hun beveiligingstaken. Vooral bij kleinere organisaties, zoals bepaalde gemeenten, is expertise op dit gebied veelal onvoldoende aanwezig. Onbewuste onbekwaamheid kan leiden tot fysieke gevolgen, maar ook tot bestuurlijke reputatieschade, financiële schade of aansprakelijkheid. Als expertise intern niet aanwezig is, is het van belang dat deze buiten de organisatie wordt gevonden.

Daarnaast moet er in ieder geval een passend wachtwoordenbeleid worden uitgevoerd. Alle standaard inlognamen en wachtwoorden van ICS/SCADA moeten worden aangepast. Anders dan in kantooromgevingen hebben administrators van ICS/SCADA doorgaans veel verschillende systemen in beheer. Het eisen van *te* lange wachtwoorden is hierdoor niet praktisch en kan de werking van het beleid ondermijnen. Wachtwoorden moeten wel zo sterk mogelijk zijn.

Personeel dat toegang heeft tot belangrijke (kritische of vitale) ICS/SCADA moet een Verklaring Omtrent Gedrag (VOG) overleggen bij indiensttreding.

**Processen**

ICS/SCADA-beveiliging moet geïntegreerd zijn in de verbeterprocessen (volgens 'Plan', 'Do', 'Check', 'Act') van de organisatie. De baselines (BIWA, BIR, BIG) schrijven voor dat ten minste eens in de drie jaar het informatiebeveiligingsbeleid wordt heroverwogen en ten minste één keer per jaar moet de opzet, het bestaan en de werking van de informatiebeveiligingsmaatregelen door verantwoordelijken formeel worden besproken.

Regie, kaders stellen en advisering vanuit de informatiebeveiligers (zoals een CISO of beveiligingsambtenaar) van de organisatie op de afwezige ICS/SCADA is essentieel voor een veilige organisatie. Daarbij is het belangrijk aan de voorkant van processen betrokken te zijn. Hoe eerder beveiliging bij inkoop- en aanbestedingen van systemen op een goede manier wordt meegenomen, hoe eenvoudiger het is om onnodige risico's te vermijden. Noodzakelijke beveiliging achteraf inbouwen, is vele malen kostbaarder dan deze direct meenemen. Voor het beveiligen van ICS/SCADA betekent dit dat de informatiebeveiligers betrokken moeten zijn bij alle projecten waar ICS/SCADA wordt toegepast, van bruggen, tunnels, verkeersregeling tot gebouwbeheersing. Informatiebeveiligers moeten hierin ook kaderstellend zijn in de relatie met externe leveranciers en externe beheerders van ICS/SCADA.

**Technologie**

Door de standaardisering en toegenomen (internet)connectiviteit gaat ICS/SCADA steeds meer op IT lijken. Hierdoor staan ICS/SCADA eveneens bloot aan dezelfde dreigingen als IT. Om kwetsbaarheden te verminderen moet goed worden gekeken of het ICS/SCADA-systeem niet te zwaar en te uitgebreid is qua hardware en functionaliteiten voor de procesbesturing die het moet uitvoeren. Uitgebreide besturingssystemen als Windows en andere software maken ICS/SCADA kwetsbaar, doordat zij net als consumenten pc's veelal niet-gepatcht of geüpdate zijn.[17] Om de inspanning voor hardening, patch management en netwerkveiligheid te verlagen, moeten systemen zo eenvoudig mogelijk worden uitgevoerd. Beveiliging moet in ieder geval fysiek en logisch gelaagd worden uitgevoerd (*defense in depth*) zodat er meerdere barrières zijn voor aanvallers.

Dataverkeer tussen ICS/SCADA enerzijds en kantoorautomatisering en internet anderzijds, moet zoveel als mogelijk worden beperkt. Als het niet anders kan, moet netwerkverkeer slechts unidirectionaal (in één richting) worden toegestaan. Uitvoering met meerdere firewalls van verschillende aanbieders, malwaredetectie en het implementeren van Intrusion Detection Systems (IDS) en monitoring (*SIEM*) zijn noodzakelijk voor netwerken.

[17] ENISA (2013a), p.1.

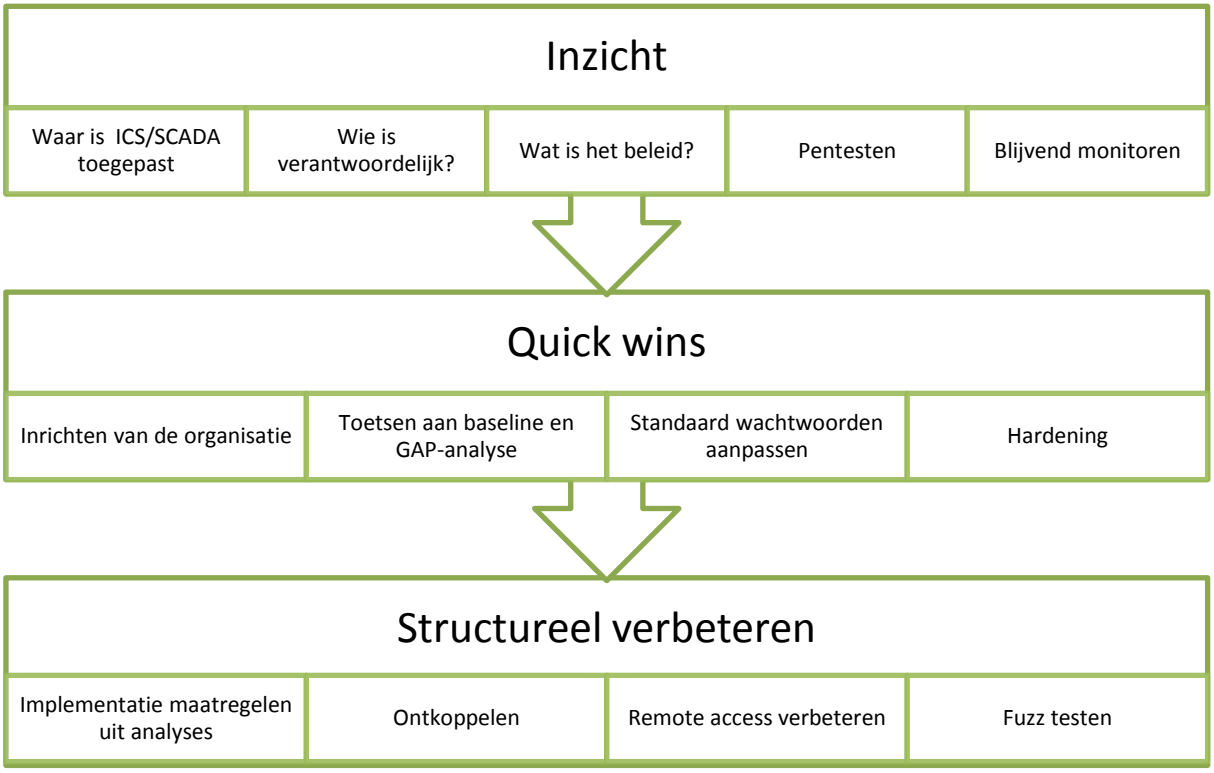
Precies in beeld krijgen waar in de organisatie ICS/SCADA aanwezig is (*asset management*), welke bedrijfsprocessen het ondersteunt en welke systemen op internet zijn aangesloten, is voor ICS/SCADA niet makkelijk vast te stellen, maar het is essentieel voor het op orde krijgen van de beveiliging. Het is zeker uitdagend als het gaat om oudere (*legacy*) systemen. Internetkoppelingen en daarbij behorende kwetsbaarheden zijn met specifieke internetzoekmachines, zoals SHODAN en Metasploit, te ontdekken. Dergelijke zoekmachines worden ook door aanvallers gebruikt om kwetsbare systemen op te sporen.

# 4 ICS/SCADA beveiliging op orde en onder controle

## 4.1 Inleiding

In dit hoofdstuk wordt een handreiking geboden voor het op orde en onder controle krijgen en houden van de beveiliging van ICS/SCADA. Hiertoe wordt moet eerst inzicht worden verkregen ten aanzien van ICS/SCADA in de organisatie. Dit wordt beschreven in paragraaf 4.2. Vervolgens moeten de eerste noodzakelijke (verbeter)stappen, de Quick wins, op het gebied van organisatie, proces en techniek worden doorgevoerd. Nadat inzicht is verkregen en de eerste stappen zijn gezet om de beveiliging te versterken, moet de beveiliging van ICS/SCADA structureel worden verbeterd zodat de beveiliging op orde en onder controle blijft.

Deze drie stappen zijn schematisch als volgt weer te geven:




## 4.2 Inzicht verkrijgen in ICS/SCADA

Veel organisaties hebben geen overzicht van aanwezige ICS/SCADA in hun processen, wie ervoor verantwoordelijk is, welke risico's de organisatie loopt en welke risico's de organisatie bereid is te nemen. Inzicht krijgen op de ICS/SCADA-omgeving is de essentiële eerste stap om de beveiliging op orde en onder controle te krijgen.

Inzicht moet worden verkregen ten aanzien van verantwoordelijkheden, processen en technische kwetsbaarheden. De eerste aan te bevelen acties om inzicht te krijgen in de kwetsbaarheid van de organisatie door ICS/SCADA zijn:

1. *Vaststellen voor welke organisatorische processen ICS/SCADA is toegepast.*

   Belangrijk is hierbij te kijken naar de functie van het proces, de betekenis van het proces voor de doelen van de organisatie en de fysieke locatie en netwerklocaties (asset management) van de ICS/SCADA.

2. *Vaststellen wie verantwoordelijk is voor de ICS/SCADA-toepassing.*

   Bij het onderzoeken van de (verdeling van) verantwoordelijkheden voor een bepaalde ICS/SCADA moet in ieder geval onderscheid worden gemaakt in de proceseigenaar, de beheerder (bv. IT of facilitair) en de verantwoordelijke voor de fysieke locatie.

3. *Ontwikkelen van organisatiebeleid ten aanzien van ICS/SCADA.*

   Door het verantwoordelijke management moeten algemeen geldende richtlijnen en maatregelen voor de omgang met ICS/SCADA worden beschreven. Beleid legt de basis voor een veilige en professionele omgang met ICS/SCADA in de organisatie. Het vastleggen van verantwoordelijkheid, en eenduidige en gedragen processen van beheer, onderhoud en inkoop voor ICS/SCADA is noodzakelijk in elke organisatie.

4. *Uitvoeren van pentesten op de ICS/SCADA-omgeving.*

   Om de zwakste plekken te identificeren en deze direct te kunnen verbeteren, is het belangrijk om penetratietesten uit te voeren op de ICS/SCADA. Aanvallen van buiten kunnen op deze manier worden voorkomen.

5. *Blijvend monitoren van de ICS/SCADA-omgeving.*

   Door voortdurende monitoring van de netwerkomgeving door netwerk managementtools en Intrusion Detection Systems (IDS) of Security Information and Event Management (SIEM) ontstaat een beter en steeds geüpdate beeld van de veiligheid van ICS/SCADA in de organisatie. Hierdoor worden voorheen nog onbekende kwetsbaarheden inzichtelijk en is verbetering mogelijk.

### 4.3 Quick wins

Als de aanwezigheid en kwetsbaarheden van ICS/SCADA en bestaande verantwoordelijkheden voor ICS/SCADA in de organisatie inzichtelijk zijn gemaakt, kunnen indien noodzakelijk de eerste verbeteringen worden doorgevoerd. Voor zover de volgende maatregelen voor ICS/SCADA nog niet zijn geïmplementeerd, is het aan te bevelen hierop zo spoedig mogelijk actie te ondernemen:

1. *Inrichten van de ICS/SCADA-organisatie*

   Voor het beheer en onderhoud van ICS/SCADA moeten vaste, eenduidige rollen worden vastgesteld en toegewezen. Ook verantwoordelijkheden voor processen met

ICS/SCADA, en verantwoordelijkheden voor risico's en de beveiliging worden in de gehele organisatie duidelijk belegd.

2. *Toetsen aan baseline en GAP-analyse*

   Een gestructureerde analyse van de risico's en een GAP-analyse ten aanzien van de genomen maatregelen en nog te de implementeren maatregelen voor ICS/SCADA verdiept het inzicht in de noodzakelijke maatregelen voor de beveiliging. Met een baselinetoets voor waterschappen en gemeenten en de Quickscan BIR voor Rijksoverheidsorganisaties kan worden vastgesteld of het basis beveiligingsniveau van de specifieke baseline voldoende is voor de beveiliging van het proces. De GAP-analyse laat vervolgens zien welke maatregelen nog moeten worden uitgevoerd. Als er geen baselinetoets en/of GAP-analyse wordt uitgevoerd, is het voor een organisatie niet mogelijk om overzicht te krijgen in de beveiligingssituatie. In het geval dat de baseline niet voldoende bescherming biedt voor het proces waarin ICS/SCADA is toegepast, moet een risicoanalyse worden uitgevoerd
   De baselines voor waterschappen, de Rijksoverheid en gemeenten schrijft voor dat deze organisaties baselinetoets (BIR: Quickscan BIR) en GAP-analyses uitvoeren.

   De Interprovinciale Baseline Informatiebeveiliging schrijft in tegenstelling tot de BIWA, BIR of BIG geen maatregelen voor die moeten worden geïmplementeerd. Provincies hebben een eigen verantwoordelijkheid om zelf passende maatregelen te identificeren en uit te voeren. Het Zelfevaluatie(instrument) Provinciale Baseline Informatiehuishouding ondersteunt provincies daarbij. Om vast te kunnen stellen welke maatregelen ten aanzien van provinciale ICS/SCADA noodzakelijk zijn, wordt aanbevolen de zelfevaluatie uit te voeren en de daaruit voortvloeiende maatregelen te implementeren.

3. *Standaard wachtwoorden vervangen*

   Alle standaard inlognamen en wachtwoorden moeten worden verwijderd van ICS/SCADA. In plaats van standaard en daardoor zeer eenvoudig te raden wachtwoorden, moet er een passend wachtwoordenbeleid worden uitgedacht en uitgevoerd. Anders dan in kantooromgevingen hebben administrators van ICS/SCADA doorgaans veel verschillende systemen in beheer. Het eisen van *te* lange, complexe wachtwoorden is in veel gevallen niet praktisch en ondermijnt de werking van het beleid. Wachtwoorden moeten zo sterk mogelijk zijn.

4. *Hardening*

   Door hardening van ICS/SCADA kunnen kwetsbaarheden relatief snel worden verminderd. ICS/SCADA worden tegenwoordig steeds zwaarder en uitgebreider uitgevoerd voor de soms relatief eenvoudig procesbesturing die het systeem als taak heeft. Dit maakt ICS/SCADA onnodig kwetsbaar door bijvoorbeeld poorten die openstaan of achterstallige updates.

Hardening is beschreven in alle baselines en zal uit de toetsing aan de baselines als noodzakelijk naar voren komen. Door de snelle beveiligingswinst die met hardening kan worden gemaakt, is het aan te bevelen de uitkomsten van de analyses niet af te wachten voordat actie wordt ondernomen.

### 4.4 Structureel verbeteren

Om de beveiliging van ICS/SCADA te borgen in de organisatie en blijvend te verbeteren zijn de volgende stappen aan te bevelen:

1. *Maatregelen uit analyses implementeren*

   De geïdentificeerde maatregelen uit de GAP-analyse (Zelfevaluatie voor provincies) en mogelijke additioneel uitgevoerde risicoanalyse moeten worden geïmplementeerd.

2. *Ontkoppelen*

   Dataverkeer tussen ICS/SCADA enerzijds en kantoorautomatisering en internet anderzijds, moet zoveel als mogelijk worden beperkt. Waarnodig moet ICS/SCADA worden ontkoppeld als niet-noodzakelijke verbindingen met kantoorautomatisering of internet bestaan. Als het niet anders kan, moet netwerkverkeer slechts unidirectionaal worden toegestaan.

3. *Remote access verbeteren*

   Als toegang op afstand noodzakelijk is voor bepaalde ICS/SCADA dan moet deze verbinding goed beveiligd zijn met VPN, netwerkmonitoring en firewalls.

4. *Fuzz testen*

   In een fuzz test worden systemen blootgesteld aan onjuiste of onverwachte data input. Vervolgens worden de gevolgen op het systeem gemonitord. Fuzz testen kan onverwachte systeem crashes of geheugen lekken onthullen die de beschikbaarheid of integriteit van ICS/SCADA kunnen ondermijnen.

## Bijlage 1: Voorbeeld ICS/SCADA beleid

### Beveiliging van ICS/SCADA

De beveiliging van ICS/SCADA is zeer belangrijk voor de beschikbaarheid, integriteit en vertrouwelijkheid van processen die worden aangestuurd door ICS/SCADA. Het niet voldoende beveiligen van ICS/SCADA kan schade toebrengen aan mensen, installaties, de omgeving en de reputatie van de organisatie. Het doel van het ICS/SCADA-beveiligingsbeleid is het op orde en onder controle hebben van de beveiliging van ICS/SCADA.

De beveiliging van ICS/SCADA voldoet aan Nederlandse wet- en regelgeving. Aanbevelingen voor de beveiliging van ICS/SCADA worden waar mogelijk uitgevoerd zoals deze door onze leveranciers en CERT's, zoals het Nationaal Cyber Security Center, worden opgesteld.

### Uitgangspunten beveiliging ICS/SCADA

De uitgangspunten voor de beveiliging van ICS/SCADA in de organisatie zijn ontleend aan de baseline informatiebeveiliging en zijn aanvullend op het informatiebeveiligingsbeleid. De volgende uitgangspunten bepalen de beveiliging van ICS/SCADA in de organisatie:

1. De beveiliging van ICS/SCADA in de organisatie maakt integraal onderdeel uit van het informatiebeveiligingsbeleid.
2. De eindverantwoordelijke voor informatiebeveiliging in de organisatie is tevens eindverantwoordelijk voor de beveiliging van ICS/SCADA.
3. De verantwoordelijkheden voor het beheer, onderhoud et cetera ten aanzien van ICS/SCADA worden zo veel mogelijk gestandaardiseerd in de organisatie.
4. Er wordt periodiek, of eerder wanneer daartoe aanleiding is, inzichtelijk gemaakt welke risico's en kwetsbaarheden de organisatie kent ten aanzien van toegepaste ICS/SCADA en welke beveiligingsmaatregelen noodzakelijk zijn. Hiertoe worden baselinetoetsen, GAP-analyses, risicoanalyses, pentesten en fuzz testen uitgevoerd.
5. Bij de inkoop van ICS/SCADA is de verantwoordelijke voor informatiebeveiliging betrokken en het uitgangspunt van *security by design* maakt deel uit van de inkoopvoorwaarden.
6. Vanwege het belang voor het beveiligen van ICS/SCADA is er specifiek aandacht voor hardening van systemen, patch management, netwerkveiligheid, monitoring en leveranciersmanagement.
7. Er bestaat zo min mogelijk dataverkeer tussen ICS/SCADA en internet, en ICS/SCADA en de kantoorautomatisering.
8. Alle standaard inlognamen en wachtwoorden moeten worden verwijderd van ICS/SCADA. Wachtwoorden moeten zo sterk mogelijk zijn.

Aldus vastgesteld door de directie van *[organisatie]* op *[datum]*

[Naam. Functie] [Naam. Functie]

## Literatuurlijst

Byres, E. (2012). *SCADA Security Basics: SCADA vs. ICS Terminology.* 5 september 2012.

ENISA (2011). *Protecting Industrial Control Systems. Recommendations for Europe and Member States [Deliverable – 2011-12-09].*

ENISA (2013a). *Can we learn from SCADA security incidents?*

ENISA (2013b). *Window of exposure… a real problem for SCADA systems? Recommendations for Europe on SCADA patching.*

Microsoft (2014). *Cyberspace 2025. Today's decisions, tomorrow's terrain.*

Nationaal Cyber Security Centrum (2012a). *Beveiligingsrisico's van on-line SCADA systemen.* Factsheet FS-2012-01. Versie 2.0 7 maart 2012

Nationaal Cyber Security Centrum (2012b). *Checklist beveiliging van ICS/SCADA systemen.* FS 2012-02. Versie 1.01. 7 maart 2012.

Nationaal Cyber Security Centrum (NCSC) (2013). *De aanhouder wint. De wereld van Advanced Persistent Threats*. Factsheet FS-2013-02C. Versie 1.3. 3 oktober 2013.

Nationaal Cyber Security Centrum (2014). *Cybersecuritybeeld Nederland. CSBN-4.*

Norea (2014). *Digitale beveiliging van industrial control systems*. 21-08-2014.

TIER-3 (2014). *Internet of Things: Enterprise Security and Control.*

Wikipedia (2014a). *Internet der Dingen*. http://nl.wikipedia.org/wiki/Internet_der_dingen. 10 september 2014.

Wikipedia (2014b). *SCADA*. http://en.wikipedia.org/wiki/SCADA. 11 september 2014.