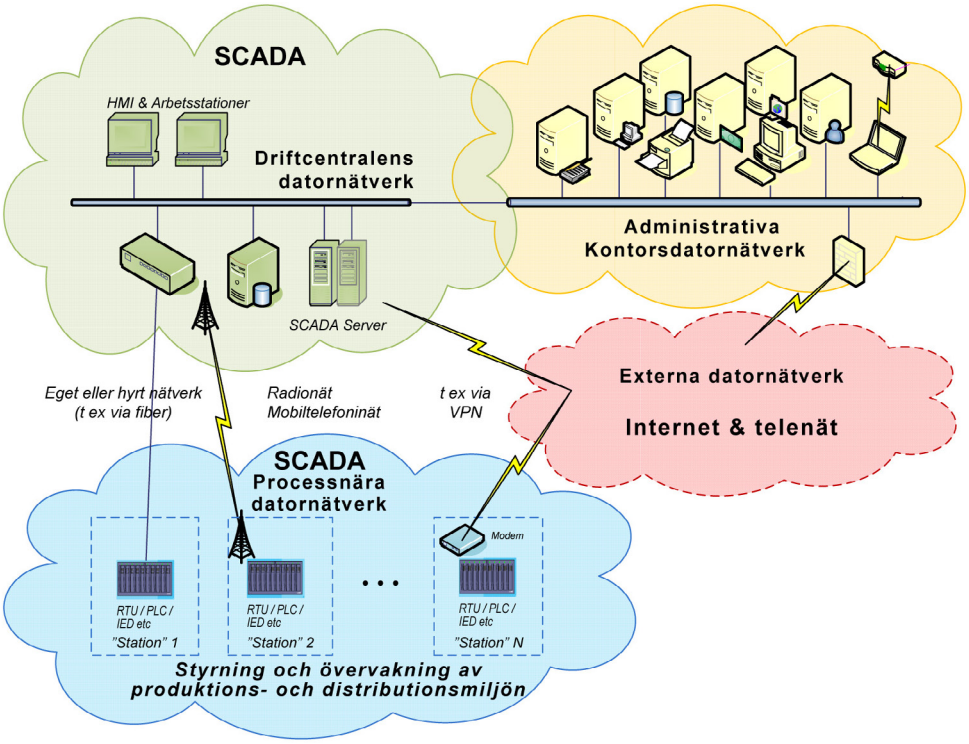
Kartläggning av SCADA-säkerhet inom svensk dricksvattenförsörjning

Erik Johansson



MSB Myndigheten för samhällsskydd och beredskap

Svenskt Vatten

Förord

Dricksvattenförsörjningen är i hög grad beroende av välfungerande industriella informations- och styrsystem. Dessa system, vilka ofta benämns SCADA-system, används vid all produktion och distribution av dricksvatten.

Sårbarheterna vid användningen av SCADA-system har under senare år uppmärksammats alltmer. Detta föranledde Svenskt Vatten samt Myndigheten för samhällsskydd och beredskap (MSB) att stödja en studie med syfte att få en överblick av SCADA-säkerheten i den svenska dricksvattenförsörjningen. En sådan överblick ger möjlighet till att kunna utforma mer relevanta råd och riktlinjer för branschen samt utgör ett utmärkt stöd vid utformning av utbildningsmaterial för kompetenshöjande insatser. Studien utgör således en grund för att kunna skapa en långsiktigt ökad SCADA-säkerhet hos den svenska dricksvattenförsörjningen.

Studien har genomförts av Tekn. Dr. Erik Johansson (författaren), Kungliga Tekniska högskolan (KTH) med finansiellt stöd från Svenskt Vatten Utveckling samt MSB. Rapporten har tagits fram i samverkan med Andreas Wiberg (Svenskt Vatten) samt Tekn. Dr. Åke J. Holmgren (MSB). Synpunkter på rapporten har även lämnats av Christina Nordensten (Livsmedelsverket). Denna sammanfattande rapport publiceras tillsammans av Svenskt Vatten och MSB. Författaren ansvarar för rapportens innehåll.

En sammanställning av sårbarheter i dricksvattenförsörjningen kan i vissa avseenden vara känslig. Valda delar av det material som tagits fram kommer därför inte göras publikt. Underlagsmaterialet ägs av Svenskt Vatten och författaren. Rapporteringen till MSB utgörs av denna rapport, inklusive konstruktion av enkäten.

Svenskt Vattens arbetsgrupp SV-SCADA har under arbetets gång bidragit med värdefullt stöd i genomförandet av studien. Ett stort tack ska också riktas till alla inom dricksvattenförsörjningen i Sverige som bidragit med erfarenheter och lagt ned tid på att svara på den enkät som ligger till grund för rapporten.

Stockholm, december 2010

Gullvy Hedenberg, Svenskt Vatten

Åke J. Holmgren, MSB

Erik Johansson, KTH

Sammanfattning

Dricksvatten utgör samhällets viktigaste livsmedel. Produktion och distribution av dricksvatten är i hög grad beroende av en vidmakthållen funktionalitet hos industriella informations- och styrsystem (s.k. SCADA-system) vilka styr, kontrollerar och övervakar den fysiska processen. När dricksvattenförsörjningen inte fungerar kan konsekvenserna för samhället bli allvarliga. Därmed utgör störningar i SCADA-system indirekt en potentiell risk för samhället.

Denna rapport bygger på en undersökning av hur informationssäkerhetsarbetet relaterat till SCADA-system bedrivs inom svensk dricksvattenförsörjning. Kartläggningen, vilken utfördes under 2009, bygger på en enkät som distribuerades till Svenskt Vattens medlemmar.

Resultaten från enkäten indikerar att kunskaperna om informationssäkerhetsfrågor hos personal inom svensk dricksvattenförsörjning är relativt låg. Studien visar att det ofta saknas ett ledningssystem för informationssäkerhet som även beaktar SCADA-system. Generellt saknas relevant utbildning och medvetenheten kring SCADA-säkerhet dessutom är kunskapen om befintliga riktlinjer och föreskrifter ofta bristfällig. Detta återspeglas även bland svaren där bara var fjärde respondent anser att nödvändig kompetens finns inom den egna organisationen. En majoritet efterlyser också ett ökat stöd inom informationssäkerhetsområdet.

Kartläggningen tydliggör hur dagens SCADA-system till en hög grad är fysiskt ihopkopplade med administrativa kontorsnätverk. SCADA-system har ofta även direkta förbindelser ut mot Internet och till leverantörer av system. Med andra ord är dricksvattenförsörjningens SCADA-system ofta sårbara då de inte är särskilt väl skyddade från omgivningen. En bidragande orsak till detta kan vara att majoriteten av organisationerna saknar en säkerhetspolicy med tydliga riktlinjer och rutiner för hur de ska genomföra risk- och sårbarhetsanalyser som tar hänsyn till de sårbarheter som existerar i SCADA-system.

Trots ökad exponering av SCADA-system på Internet, visar studien få tecken på att dricksvattenanläggningarna har varit utsatta för IT-relaterade incidenter. En möjlig bakomliggande orsak till detta kan dock vara att majoriteten av de tillfrågade uppger att det inom organisationen saknas system och processer för att korrekt upptäcka intrång och systematiskt hantera dessa typer av incidenter.

Baserat på resultaten från kartläggningen föreslås att ett antal insatser genomförs för att höja den generella medvetenheten, utbildningsnivån och kompetensen inom området.

Summary

The supply of drinking water, which represents society's most important provision, is largely dependent on maintaining the functionality of industrial information and control systems (also known as SCADA systems). If the drinking water supply fails, the societal consequences can be severe. Disturbances in SCADA systems in the production and distribution of drinking water are therefore indirectly a security risk to the society.

This report is based on a survey of SCADA security in the drinking water sector. The survey was conducted in 2009 through a questionnaire that was distributed to all Swedish drinking water suppliers.

The results from the survey indicate that the level of information security among the Swedish drinking water suppliers is relatively low. The survey shows the absence of an Information Security Management System, which takes into account the SCADA systems. In general, organizations lack relevant training and the awareness of existing guidelines is inadequate. For instance, only one in four respondents believes that the necessary skills and knowledge exist within their own organization. A majority of respondents would appreciate more support from The Swedish Water & Wastewater Association (SWWA) regarding information security for SCADA-systems.

The survey demonstrates how today's SCADA systems to a large extent are physically connected with the administrative office network. In many cases, SCADA systems have direct links to the Internet and remote connections to the SCADA system vendors. In other words, drinking water suppliers with vulnerable SCADA systems are not well protected from the external environment. The drinking water organizations often lack an information security policy and procedures for how to conduct risk and vulnerability analysis that takes into account the vulnerabilities that could exist in their SCADA systems.

Despite the increased exposure of SCADA system towards the Internet, the study does not indicate that drinking water facilities have been exposed to IT-related incidents. A possible reason for this might be that the majority of respondents state that their organizations do not have systems and processes in place in order to correctly detect intrusions and systematically deal with incidents.

Based on the results of the survey, efforts should be undertaken to raise the general level of SCADA security awareness, education and competence in the drinking water sector.

Innehåll

Figurförteckning

Förkortningar

ANSI	American National Standards Institute
FIDI-SC	Forum för Informationsdelning-SCADA
FOI	Totalförsvarets forskningsinstitut
FTP	File Transfer Protocol
HMI	Human Machine Interface
HTTP	Hypertext Transfer Protocol
IDS	Intrusion Detection Systems
IEC	International Electrotechnical Commission
IP	Internet Protocol
IPS	Intrusion Protection System
IT	Information Technology
KBM	Krisberedskapsmyndigheten
KTH	Kungliga Tekniska högskolan
LAN	Local Area Network
NICC	Dutch National CyberCrime Infrastructure
NIST	National Institute of Standards and Technology
MAC	Media Access Control
MITM	Man-in-the-Middle
MSB	Myndigheten för samhällsskydd och beredskap
RPS	Rikspolisstyrelsen
SCADA	Supervisory, Control, and Data Aquisition
SIK	Säkerhet i kontrollsystem
SLV	Statens Livsmedelsverk
SV	Svenskt Vatten
SVU	Svenskt Vatten Utveckling
SÄPO	Säkerhetspolisen

1 Inledning

1.1 Bakgrund

1.1.1 Ökad effektivisering i dricksvattenförsörjningen

Det finns en drivkraft att i allt högre grad använda datorbaserad informations- och kommunikationsteknik för att förbättra service, främja kvaliteten och öka effektiviteten inom den svenska dricksvattenförsörjningen. Denna datorisering sker i en snabb takt och pågår inom flera olika områden. Ett område som nu förändras är processnära industriella informations- och styrsystem, vilka i denna rapport benämns SCADA-system. Dessa SCADA-system har traditionellt varit helt isolerade från omgivningen men med hjälp av datorbaserade komponenter kan dessa allt lättare integreras med andra IT-system så att verksamheten kan effektiviseras. Ett exempel på effekten av en sådan effektivisering är att dricksvattenförsörjningen idag kan hanteras av betydligt färre individer än för bara tio år sedan. En operatör kan idag övervaka och fjärrstyra alla vattenverkets pumpar, ventiler och ibland hela vattenledningsnät från en central arbetsplats. En arbetsplats som idag inte längre alltid behöver vara bunden till en välbevakad fysiskt skyddad driftcentral utan numera kan utgöras av en bärbar dator i hemmet.

Datoriseringen möjliggör även digitalisering av informationsunderlag, såsom ledningskartor och systembeskrivningar, vilket ökar tillgängligheten. Kommunikationen mellan datorer sker numera allt oftare över nätverk som dessutom sträcker sig långt utanför det lokala vattenverkets egna lokaler.

En stark drivkraft bakom datoriseringen i produktionen och distributionen av dricksvatten är möjligheterna till ökad effektivisering med tillhörande kostnadsbesparingar.

1.1.2 Nya risker med ökad datorisering

Att datorbaserade system kan manipuleras på olika sätt är allmänt känt. Om en otillbörlig manipulering sker av de alltmer datorbaserade processnära SCADA-systemen kan detta medföra att samhället får en sämre dricksvattenförsörjning. Risker som kan följa av den ökade användningen av datorbaserade SCADA-systemen har oftast inte beaktats tidigare. För att hantera dessa risker och minimera framtida störningar i dricksvattenförsörjningen krävs att informationssäkerhetsarbetet bedrivs på ett ändamålsenligt och effektivt sätt.

Dricksvattenförsörjningen har dock länge saknat gemensamma riktlinjer för hur informationssäkerhetsarbetet relaterat till de processnära SCADA-systemen ska bedrivas. Det finns därför ett

behov att få en tydligare bild av hur det aktuella informationssäkerhetsarbetet bedrivs inom den kommunala dricksvattenförsörjningen.

1.2 Intressenter

1.2.1 Svenskt Vatten

Svenskt Vatten företräder VA-verken och VA-bolagen i Sverige. Medlemmarna i Svenskt Vatten levererar dricksvatten och tar emot avloppsvatten från mer än åtta miljoner människor. De är därmed Sveriges viktigaste livsmedelsproducenter och miljövårdsföretag. Svenskt Vatten samlar in och bearbetar erfarenheter, initierar och genomför utredningar, stöder forsknings- och utvecklingsarbete samt utarbetar råd och anvisningar (SV 2009).

Ett av Svenskt Vattens mål är att bidra till ett ökat säkerhetsmedvetande via aktiv kunskapsspridning, kompetensförsörjning, intressebevakning, kommunikation och samverkan. Därför har Svenskt Vatten bildat en arbetsgrupp, kallad SV-SCADA, vars övergripande mål är att öka medvetenheten om sårbarheter i SCADA-system samt att på sikt förmedla konkreta råd och anvisningar om hur det datorrelaterade skyddet hos dricksvattensektorn kan förbättras. SV-SCADA har inledningsvis bestått av representanter från följande organisationer: Svenskt Vatten, KTH, Norrvatten, Stockholm Vatten, MittSverige Vatten, VA SYD, Gästrike Vatten samt Ludvika kommun. Mer om SV-SCADA framgår på Svenskt Vattens hemsida (SV 2009).

Svenskt Vatten Utveckling (SVU) är kommunernas eget FoU-program om kommunal VA-teknik. Verksamheten finansierar tillämpad forskning och utveckling som är av intresse för Svenskt Vattens medlemmar, därav det finansiella stödet av detta projekt. Målet för SVU är att främja utvecklingen av ny kunskap inom områdets alla delar, stödja branschens behov av kompetensförsörjning samt se till att framtagen kunskap sprids (SVU 2009).

1.2.2 Myndigheten för samhällsskydd och beredskap

Myndigheten för samhällsskydd och beredskap (MSB) har till uppgift att utveckla och stödja samhällets förmåga att hantera olyckor och kriser samt bidrar till att samhället förebygger händelser och att beredskap finns när de inträffar. MSB har även till uppgift att stödja och samordna arbetet med samhällets informationssäkerhet samt analysera och bedöma omvärldsutvecklingen inom området (MSB 2010a).

MSB (och dess föregångare KBM) har arbetat aktivt med SCADA-säkerhet sedan 2005 och har som en del av detta arbete bland annat etablerat ett forum för informationsdelning avseende informationssäkerhet i SCADA-området (FIDI-SC). FIDI-konceptet baseras på riktlinjer och erfarenheter från brittiska Centre for the Protection of National Infrastructure (CPNI) och innebär att myndigheter och industri delar information om risker och sårbarheter. Syftet med samverkan är bland annat att skapa en mekanism där en enskild organisation kan ta lärdom av andras erfarenheter, misstag och framgångar för att höja sin egen säkerhetsnivå (CPNI 2010; MSB 2007).

1.3 Denna rapport

1.3.1 Syfte

Syftet med rapporten är att redovisa resultatet av den kartläggning av SCADA-säkerhet inom svensk dricksvattenförsörjning som genomförts med stöd av Svenskt Vatten Utveckling och MSB.

Det övergripande syftet med att genomföra kartläggningen var att ta fram kunskap för att få möjlighet att prioritera eventuella insatser som kan behövas för att utveckla relevanta råd och riktlinjer, kompetenshöjande utbildningar och seminarier för att öka säkerheten i SCADA-system. Dessutom ger ökad kunskap en grund för fördjupad förståelse som kan visa var ytterligare forskning är nödvändigt. Ytterligare ett syfte med att genomföra en kartläggning var att undersöka vad som är praxis inom branschen, dvs. vilka metoder/processer som används.

Det långsiktiga syftet med MSB:s verksamhet inom området är en ökad samverkan mellan privata och offentliga aktörer i syfte att öka säkerheten i SCADA-system i samhällsviktiga verksamheter. Studien som redovisas i denna rapport utgör ett tillämpningsexempel i arbetet med ta fram en metodik för att kartlägga arbetet med säkerhet i SCADA-system hos små och medelstora operatörer av samhällsviktig verksamhet.

1.3.2 Genomförande

Initiativtagare till att genomföra en kartläggning var Svensk Vatten arbetsgrupp SV-SCADA. I deras arbete framkom att det saknades grundläggande studier avseende informationssäkerhet i SCADA-system inom dricksvattenförsörjningen. Tillsammans med resultaten från en genomförd praktisk utvärdering av ett större svenskt vattenverk, och ett allt större internationellt engagemang på området, framträdde ett allt tydligare behov av att förvärva ytterligare kunskap. För att genomföra denna kartläggning

behövdes ekonomiskt stöd vilket erhölls från både MSB samt Svenskt Vatten Utveckling, se vidare (MSB 2009; SV 2009; SVU 2009).

1.3.3 Rapportstruktur

Rapporten utgör den officiella sammanställning av metodiken samt de övergripande resultaten från den kartläggningsstudie som initierades under 2009.

Rapporten inleds med en kort bakgrund till området och de drivkrafter som motiverat studien. Därefter beskrivs hur kartläggningen har genomförts samt vilka åtgärder som vidtagit för att minimera dess felkällor.

I nästa kapitel återfinns en kortfattad sammanställning av allmän bakgrundsinformation från respondenterna. Resultaten av övriga frågor sammanfattas endast övergripande. I de följande kapitlen återfinns en kortfattad diskussion samt förslag till fortsatt arbete.

Därutöver består rapporten av ett antal utvalda referenser samt två bilagor. I bilagorna återfinns en kopia av enkäten och dess följebrev.

2 Metodfrågor

2.1 Kartläggningens upplägg

Kartläggning utfördes genom att en enkät skickades ut via brev till VA-ansvariga i Sveriges kommuner under 2009.

För att behålla en hög sekretessnivå skickades enkäten ut i pappersform. Vid utskicket erhölls ett personligt följebrev (se Bilaga 1) med tydliga instruktioner samt ett i förväg adresserat svarskuvert. Detta gjordes framförallt för att undvika att få in elektroniska kopior av enkätsvaren. Dessa skulle med stor sannolikhet annars ha skickats in via e-post. Denna informationskanal ansågs dock inte ha tillräckligt hög säkerhet för den information som ämnades samlas in.

Enkäten efterfrågade information som kan vara känslig varför det var av stor vikt att respondenterna kände förtroende för att deras svar skulle komma att hanteras på ett tillförlitligt sätt. För att förtydliga att svar som lämnades i enkäten inte skulle komma att användas för att peka ut enskilda respondenter, tydliggjordes i enkäten att insamlingen skedde på ett kontrollerat sätt och att inkomna svar anonymiserades. Enkäten inleddes med texten:

”Alla svar kommer att behandlas konfidentiellt! All sammanställning, analys och rapportering kommer att ske anonymiserat och kommer inte spåras till någon individuell organisation. ”

För att respondenterna även själva skulle inse att den ifyllda enkäten innehöll kritisk information fortsatte informationstexten i enkäten med att ge följande uppmaning till respondenterna:

”OBS! Er ifyllda enkät måste hanteras förtroligt då den kan komma att innehålla känsliga uppgifter!”

2.2 Enkätens struktur

Underlaget för enkäten är baserat på författarens egna erfarenheter från tidigare genomförda praktiska utvärderingar av SCADA-säkerhet inom dricksvattenförsörjningen samt aktuella nationella och internationella riktlinjer, standarder och föreskrifter m.m. (ANSI 2004; Cegrell 1994; CORE 2008; CPNI 2009; ISO/IEC 2005a; ISO/IEC 2005b; Johansson 2005-2009; KBM 2006-2008; MSB 2009a; MSB 2009b; NIST 2007; SLV 2003; SLV 2007). Arbetet har hämtat inspiration från en liknande studie som genomfördes i Holland av TNO Defence, Security and Safety på uppdrag av NICC (Dutch National Cyber Crime Infrastructure) (NICC 2008).

Ett stort antal relevanta frågeställningar växte fram. Enkäten blev omfattande och kom slutligen att omfatta ett sextiotal olika frågeställningar. Enkätens frågeställningar fördelas i olika områden, se bilaga 2. Den övergripande strukturen omfattande följande områden:

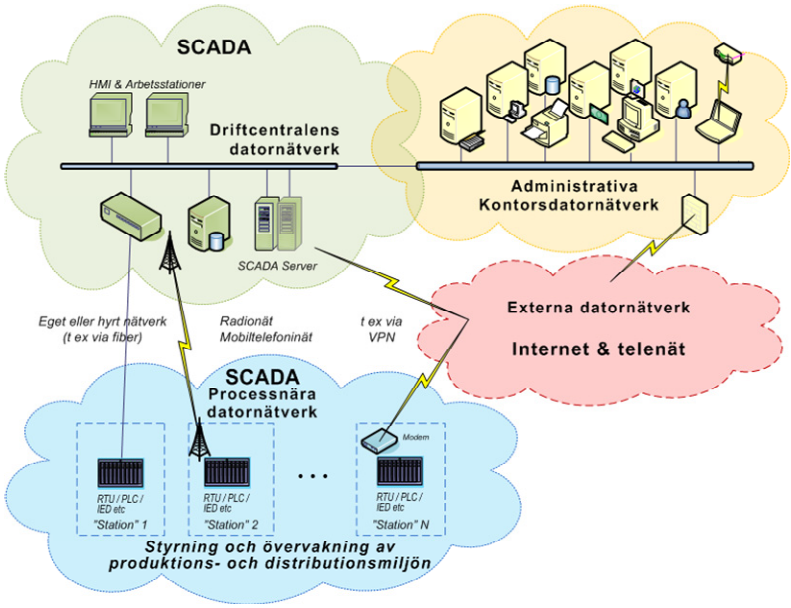
- Referensmodell och terminologi (Avsnitt A)
- Bakgrundsinformation kring respondent och verksamheten (Avsnitt B)
- Tekniska aspekter (Avsnitt C)
- Organisatoriska aspekter (Avsnitt D)
- Hot- och riskaspekter (Avsnitt E)
- Övriga aspekter (Avsnitt F)

Därutöver fanns avsnitt som behandlade instruktioner till respondenten samt ev. kontaktuppgifter och även utrymme för synpunkter.

2.3 Referensmodell

För att förtydliga terminologin som användes i enkäten försågs respondenterna med en referensmodell i enkätens inledning (Avsnitt A), se Figur 2-1 nedan. I denna referensmodell skiljs framförallt på följande fyra områden:

- driftcentralens datornätverk, (grönfärgade molnet),
- processnära datornätverk, (blåfärgade molnet),
- administrativa kontorsdatornätverk, (gulfärgade molnet), samt
- externa datornätverk, (rödfärgade molnet).



Figur 2-1. Referensmodell för övergripande beskrivning av SCADA-miljön.

Notera att i enkäten (såväl som i denna rapport) används termen SCADA som ett övergripande samlingsbegrepp för all form av IT-baserad processkontrollstyrning.

SCADA återfinns därför i såväl driftcentralens datornätverk (gröna molnet) som i produktions- och distributionsmiljön (blå molnet). Övriga områden som ofta interagerar med SCADA-system är datorsystem i det administrativa kontorsnätverket (gula molnet) samt datorsystem från underleverantörers tjänster som befinner sig på externa nätverk utanför er kontroll (röda molnet), se Figur 2-1 ovan.

2.4 Felkällor och analysproblem

Det finns flera möjliga felkällor i denna form av undersökning. Exempelvis kan svar medvetet eller omedvetet förvanskas eller att felaktiga svar lämnas på grund av bristande förståelse för aktuell frågeställning. Detta kan i sin tur bero på otillräcklig kompetens hos respondent och/eller hos frågeställaren (som då leder till otydliga formuleringar).

Att enkäten skickades ut i pappersform med ett personligt följebrev gav möjlighet att tydligare motivera vad som förväntades av respondenterna, exempelvis avseende kompetens och erfarenhet, för att ytterligare minimera dessa felkällor. För att enkätsvaren inte skulle begränsas av respondents kompetens och förmåga uppmanades de att säkerställa kvaliteten på svaren genom att arbeta med enkäten tillsammans i grupp där flertalet kompetenser var samlade.

Hanteringen av enkätsvaren har skett på ett kontrollerat sätt. Enbart betrodda personer har haft tillgång till svarsmaterialet. Ett omfattande arbete har lagts ned på att samla in och anonymisera underlaget till denna rapport – dvs. på den manuella hanteringen av enkäterna. Då enkäten genomfördes i pappersform, bestod av en stor mängd frågor och samtidigt fick en hög svarsfrekvensen, kom arbetet med att göra sammanställningen och analysera svaren att ta betydligt längre tid i anspråk än vad som förutsetts.

Det är ur många avseende svårt att genomföra en bra undersökning av det här slaget. Att undersöka komplexa problem som berör både tekniska och administrativa säkerhetsrelaterade frågeställningar med hjälp av en enkät kan knappast bli helt komplett. Likväl är den bedömning som görs här att resultaten som presenteras i nästa kapitel kan ses som en god indikation på den aktuella statusen när det gäller SCADA-säkerhet i vattensektorn.

3 Resultat

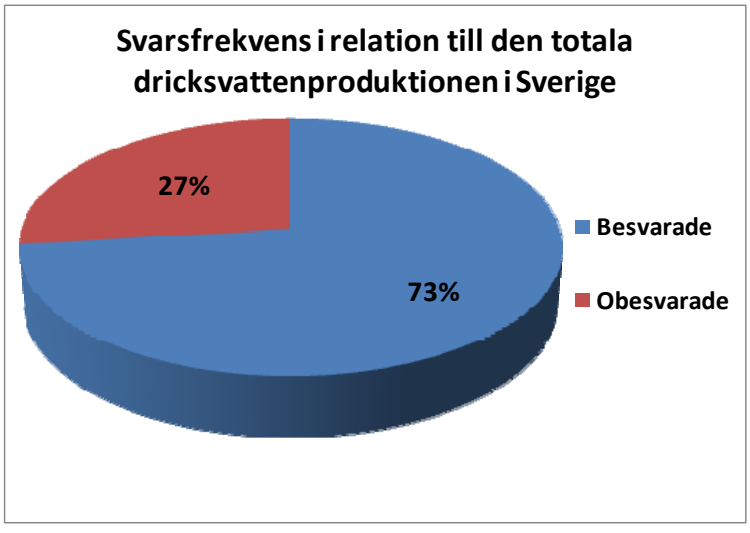
3.1 Förutsättningar för resultatredovisningen

I detta kapitel redovisas kortfattat resultaten från enkätundersökningen Inledningsvis redogörs för svarsfrekvens och den bakgrundsinformation som gav i enkäten (Avsnitt B). Resultaten från de övriga fyra avsnitten, C-F, i enkäten – ”Tekniska aspekter”, ”Organisatoriska aspekter”, ”Hot- och riskaspekter”, samt ”Övriga aspekter” – redovisas endast i en sammanfattad form. Det detaljerade arbetsmaterialet, vilket ägs av Svenskt Vatten och författaren, utgör dock ett underlag som kommer att användas för framtagning av checklistor, rådgivande dokument samt vid kompetensutveckling av operatörer.

3.2 Svarsfrekvens

Fram till årsskiftet 2010 hade 87 stycken VA-organisationer besvarat enkäten.

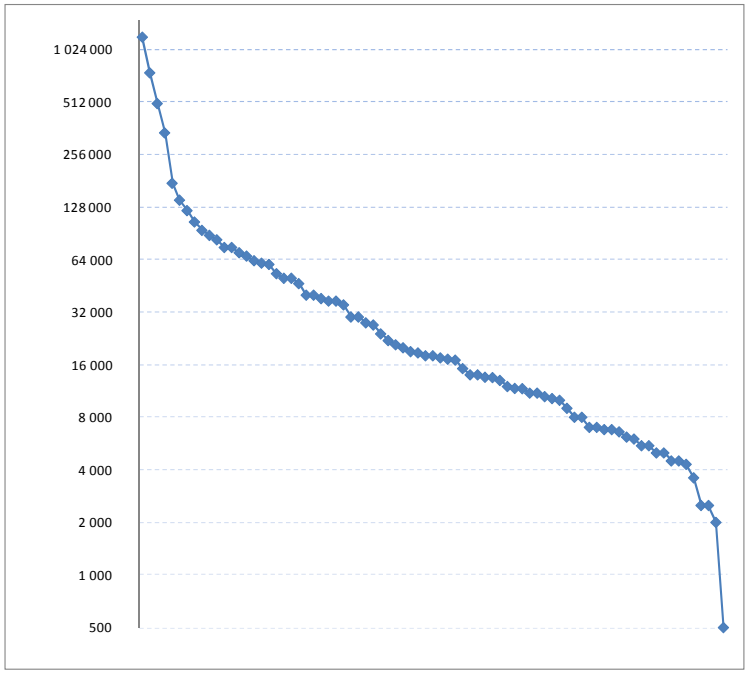
Baserat på uppgifter om storleken på anläggningen kan vi få fram att dessa enkätsvar motsvarar en samlad dricksvattenproduktion på mer än två miljoner kubikmeter per dygn. I relation till den totala dricksvattenproduktionen i Sverige motsvarar dessa enkätsvar med andra ord en svarsfrekvens på mer än 73 % av den totala dricksvattenproducerande kapaciteten i Sverige, se Figur 3-1 nedan.



Figur 3-1. Svarsfrekvens i relation till dricksvattenproduktionen i Sverige.

Enkätsvaren representerar således dricksvattenförsörjningen till mer än fem miljoner personer (med andra ord ca 64 % av Sveriges befolkning).

Studeras fördelningen av enkätsvaren ur ett storleksperspektiv visar Figur 3-2 nedan ett fåtal riktigt stora dricksvattenproducenter och en stor mängd små och mellanstora anläggningar.



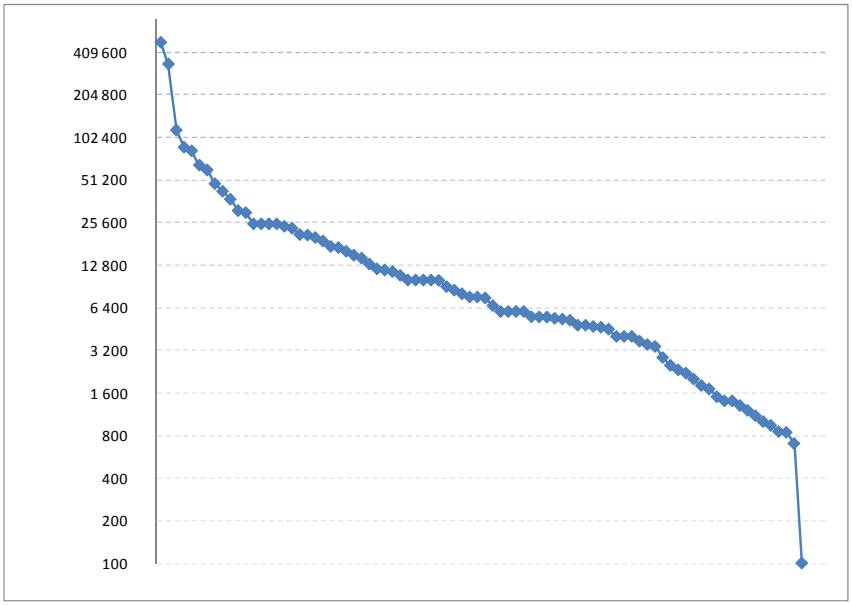
Figur 3-2. Enkätsvarens fördelning utifrån storlek, här visat med antalet personer (längs y-axeln) i relation till respektive vatten-producent/distributör (x-axeln).

I analysen av enkätsvaren gjordes därför en indelning av dricksvattenproducenternas storlek i följande tre grupper:

1) Stora enheter:	> 100 000 personer
2) Mellanstora enheter:	10 000 till 100 000 personer
3) Små enheter:	< 10 000 personer

I analyser av resultat har i flera fall en uppdelning gjorts utifrån denna storleksindelning.

I följande Figur 3-3 nedan beskrivs storleksfördelningen utifrån produktionskapacitet (m^3/dygn).

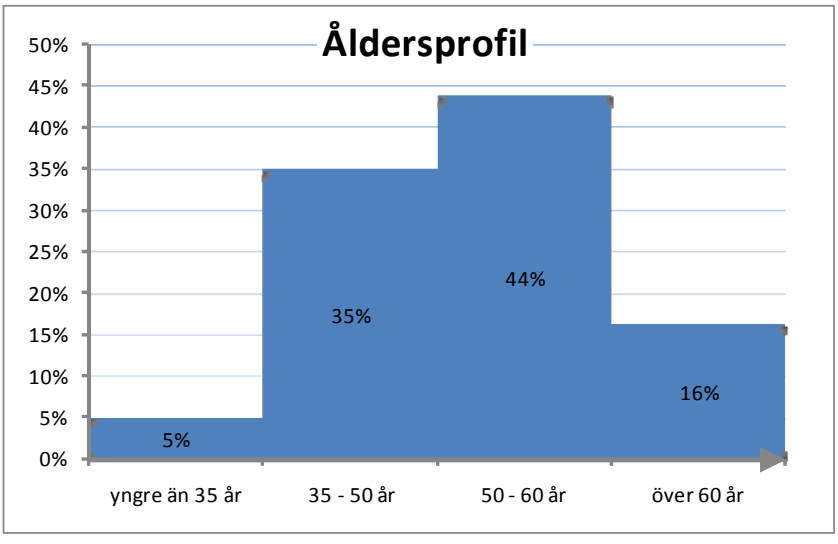


Figur 3-3. Enkätsvarens fördelning utifrån produktionskapacitet, här visat med kapacitet i m^3/dygn (längs y-axeln) i relation till respektive vattenproduktion/distributionsenhet (längs med x-axeln).

3.3 Resultat avsnitt B – Bakgrundsinformation

3.3.1 Åldersprofil

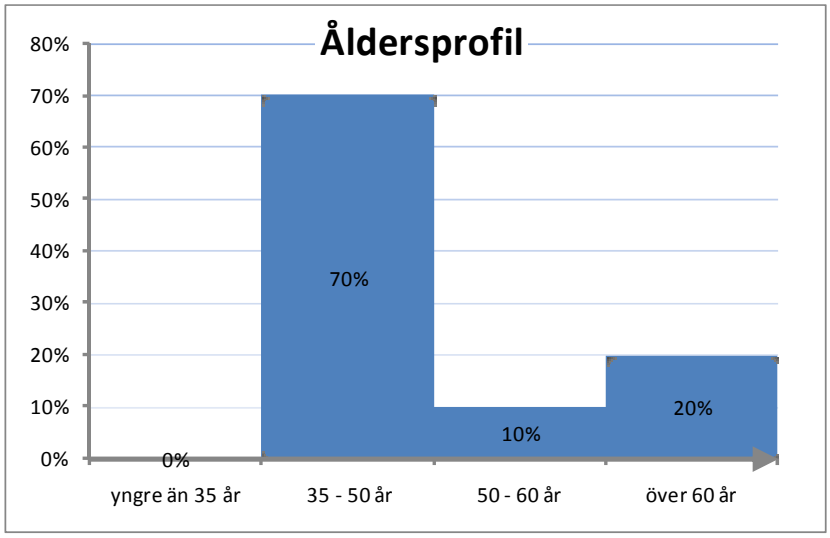
Respondenternas åldersprofil visas i Figur 3-4 nedan.



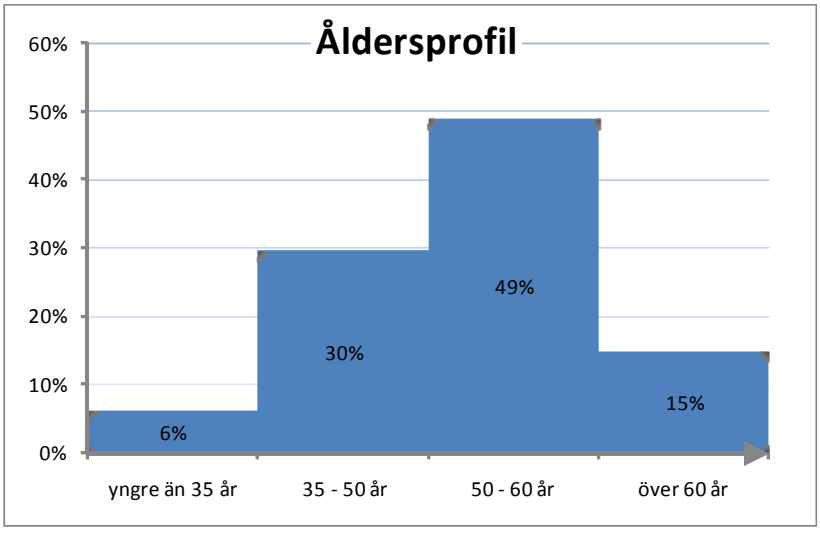
Figur 3-4 Åldersprofil för respondenter (totalt).

Åldersprofilen indikerar att det idag finns en mycket kompetent och erfaren organisation ute på vattenverken. En mycket stor andel av respondenterna är 50 år eller äldre.

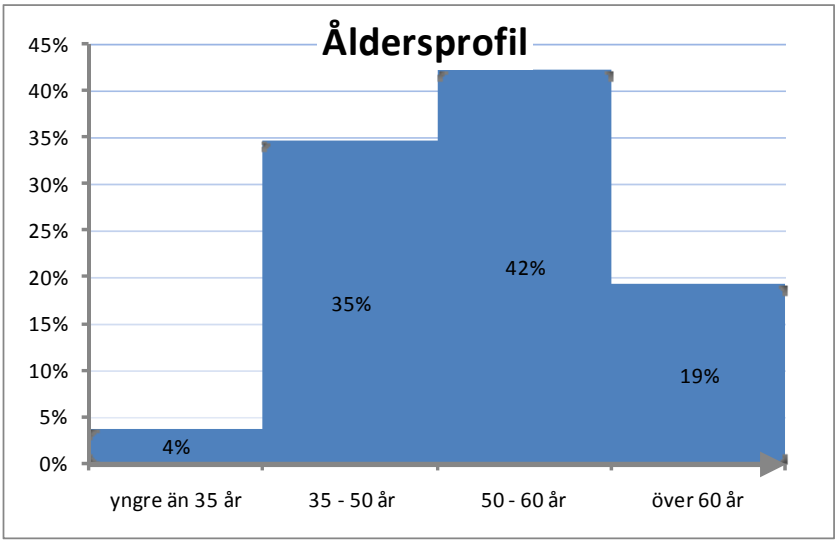
De tre följande figurerna, Figur 3-5 till 3-7, illustrerar åldersprofilerna i de tre olika storleksgrupperna för dricksvattenverken.



Figur 3-5. Åldersprofil för de största dricksvattenverken.



Figur 3-6. Åldersprofil för de mellanstora dricksvattenverken.



Figur 3-7. Åldersprofil för de minsta dricksvattenverken.

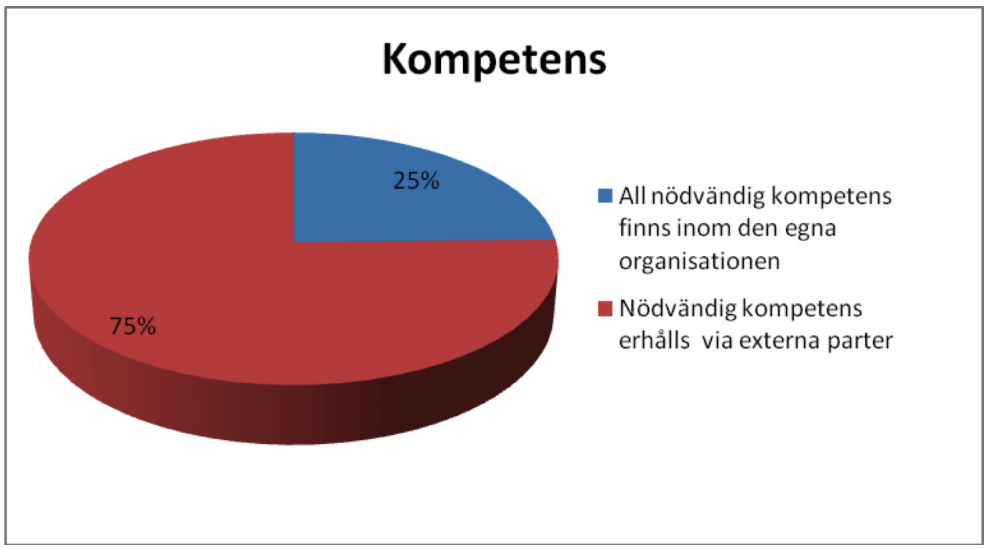
Notera att säkerhetsarbetet ofta baseras på en stor erfarenhet och kunskap om processen. Stora pensionsavgångar framöver kan snabbt vända ålderprofilen och orsaka svårigheter i säkerhetsarbetet, om inte insatser för kompetensöverföring genomförs i god tid.

3.3.2 Kompetensbehov inom organisationen

I bakgrundsinformationen ombads respondenterna att ange om de ansåg att det inom organisationen saknades kompetens för att på bästa sätt ställa krav, utveckla, underhålla, vidmakthålla och höja informationssäkerheten i SCADA-systemen.

En fjärdedel ansåg att all nödvändig kompetens fanns inom den egna organisationen, se Figur 3-8. Merparten erhåller nödvändig kompetens genom att anlita externa underleverantörer eller kommunens IT-avdelning. Respondenterna tillfrågades även om vilka områden där de anser sig sakna kompetens och följande är exempel på de svar som gavs:

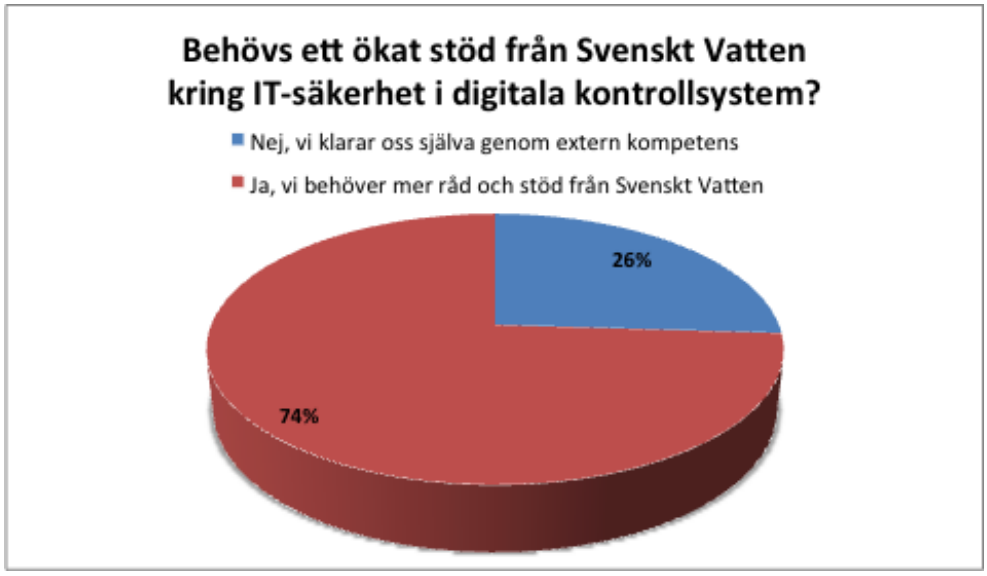
- Datasäkerhet/IT-säkerhet
- Brandväggs och nätverkskonfigurering
- Avtal med IT-konsulter
- Skriva upphandlingsunderlag
- Programmering av styr och reglerutrustning
- Säkerställa IT-säkerheten mot externa anslutningar
- Drift och utveckling av SCADA-system
- Lagar
- Kopplingar till verksamhetens IT
- Säkerhetsfrågor beträffande information
- Tydliga roller i informationssäkerhet



Figur 3-8. Aktuellt kompetensbehov inom organisationen (totalt).

3.3.3 Behov av ökat stöd från Svenskt Vatten

En frågeställning i enkäten handlar om respondenterna anser att branschorganet Svenskt Vatten framöver bör erbjuda sina medlemmar ett ökat stöd inom SCADA-säkerhetsområdet.



Figur 3-9. En majoritet av medlemmarna anser att Svenskt Vatten bör erbjuda mer råd och stöd kring IT-säkerhet i digitala kontrollsystem.

Resultaten påvisar att Svenskt Vattens medlemmar gärna ser att det erbjuds ett utökat stöd kring IT-säkerhet i SCADA-system, se Figur 3-9. Detta utgör det övergripande målet med den av Svenskt Vatten startade arbetsgruppen SV-SCADA.

3.3.4 Stöd som efterfrågas

För att försöka belysa inom vilka områden som respondenterna ser att Svenskt Vatten behöver ge ökat stöd ställdes en fråga om detta.

Ingen enskild fråga utmärkte sig utan respondenterna söker stöd på bred front. Nedan listas områden i rangordning:

1) Råd och riktlinjer för hur praktisk utvärdering av SCADA-system kan genomföras.
2) Förmedla kompetens om nya hot och risker samt identifierade sårbarheter.
3) Kompetenshöjande insatser som utbildningar och seminarier.
4) Förmedla erfarenheter från upphandlingar och underhåll
5) Bearbeta leverantörer så att dessa ökar sina insatser för höjd SCADA-säkerhet.

3.4 Resultat avsnitt C – Tekniska aspekter

Av resultaten från enkäten kan vi konstatera att dagens SCADA-system ofta har används under längre tid och att de baseras på en, i många avseenden, föråldrad teknik.

Vidare uppger merparten av respondenterna att anläggningarna inte har en uppdaterad dokumentation. Det saknas en dokumentation som på ett tydligt sätt visar alla delsystem och komponenters kopplingar och beroenden, inte bara till varandra utan även till andra IT-system, nätverk eller andra resurser i verksamheten.

En av anledningarna till att det finns en bristfällig kunskap om vilka kopplingar och beroenden som finns i anläggningarna kan bero på att det inte sker regelbundna utvärderingar av detta.

Samtidigt som dokumentationen i många fall anses bristfällig framgår det av enkätsvaren att allt fler av anläggningarnas SCADA-system integrerats (kopplas ihop) med kontorsnätverk för att möjliggöra en effektivare och mer kostnadseffektiv drift. Tidigare har dessa system varit isolerade från omvärlden men vid denna studie framkommer det att bara en minoritet av respondenterna ansåg att deras SCADA-system var fysiskt separerat från kontorsnätverk och Internet.

När det gäller det fysiska skyddet är medvetenheten relativt sett betydligt högre än vad gäller IT-säkerheten. En majoritet har staket och låsta dörrar som omger både SCADA-system och dess komponenter (kontrollrummet/driftcentralen och andra känsliga lokaler som exempelvis pumpstationer). Däremot har relativt få anläggningar genomgått en härdningsprocess av sina SCADA-system där oanvända tjänster och dataportar har avaktiverats. Därutöver tillåts i en majoritet av anläggningarna att extern underhållspersonal ges möjlighet att koppla in sin utrustning (exempelvis en bärbar dator) till SCADA-systemet och dess nätverk.

3.5 Resultat avsnitt D – Organisatoriska aspekter

Trots att informationssäkerhetsstandarder (t ex ISO/IEC 27002) påtalar att det är viktigt att etablera tydliga roller och ansvar för informationssäkerheten i en verksamhet så uppger cirka 40 % av de tillfrågade att detta saknas. En klar majoritet av respondenterna uppger att det saknas en informationssäkerhetspolicy som omfattar SCADA-system. Vidare saknar de flesta en process för att löpande kartlägga och genomföra riskanalyser av SCADA-system.

Fler än två tredjedelar av respondenterna uppger att personal med tillgång till SCADA-system saknar grundläggande utbildning i informationssäkerhet. Bristande utbildning och en låg medvetenhet kring säkerhetsrelaterade frågeställningar återspeglas även i det faktum att det saknas informationssäkerhetsmässiga krav i merparten av de upphandlingar som genomför av SCADA-system, datornätverk och de tjänster som kontrakteras.

För att belysa om insiders kan utgöra ett hot mot verksamheten ställdes frågan om det genomförs bakgrundskontroller på personal och entreprenörer, vilka ges tillgång till kritiska SCADA-system eller till de lokaler där dessa finns placerade. Ytterst få respondenter svarade att man genomför dessa kontroller.

Vi konstaterade tidigare att befintlig dokumentation oftast var bristfällig. Detta kan även hänföras till att respondenterna pekar på att det oftast saknas en formaliserad process för att hantera förändringar i SCADA-system samt förändringar i utrustning och/eller programvara.

En majoritet saknar en kontinuerlig detektering av möjliga intrång (t.ex. regelbunden genomgång av loggar och/eller via automatiserade verktyg). Merparten saknar dessutom en incidenthanteringsplan som beskriver hur IT-relaterade incidenter ska rapporteras och vem som ska göra vad.

De kontinuitetsplaner som finns etablerade omfattar framförallt en säker backup av konfigurationsdata som lagras på en avsides belägen plats. Näst intill samtliga respondenter har backuper på konfigurationer och data som gör att system i teorin snabbt kan återställas.

Näst intill samtliga respondenter anser att det är möjligt att köra vattenverket helt ”manuellt” (dvs. utan stöd från några SCADA-system).

3.6 Resultat avsnitt E – Aspekter på hot och risker

Allt oftare förekommer artiklar om sårbarheter och hot mot datorbaserade system i samhället. I enkäten fanns därför en tabell där respondenterna ombads ge sin syn på vilka hot och risker som de anser att SCADA-system kan komma att utsättas för. Respondenternas rangordning av de hot som listades i tabellen blev följande:

1) Anställda som omedvetet begår felaktigheter
2) Oriktade attacker (t ex via datorvirus)
3) Anställda som medvetet begår felaktigheter
4) Terrorism/vandalism med ”politiska” motiv
5) Riktade attacker i utpressningssyfte
6) Före detta anställdas hämnd/illvilja

När det gäller hot som redan inträffat var det 15 % som ansåg att de redan råkat ut för att anställda omedvetet begått felaktigheter. Totalt uppgav 7 % att de blivit utsatt för oriktade attacker (t.ex. via datorvirus).

Endast en fjärdedel av respondenterna angav att SCADA-systemen och deras nätverk utgjorde en del av den regelbundna affärsmässiga riskanalys som organisationen genomför. Av dessa var merparten de stora vattenverken.

Cirka åtta procent av respondenterna uppgav att de har haft IT-relaterade säkerhetsincidenter i sina SCADA-system och nätverk de senaste åren. Denna siffra får dock ställas i relation till att de flesta anläggningar saknar någon form av incidenthanteringsplan eller funktioner för detektering av intrång.

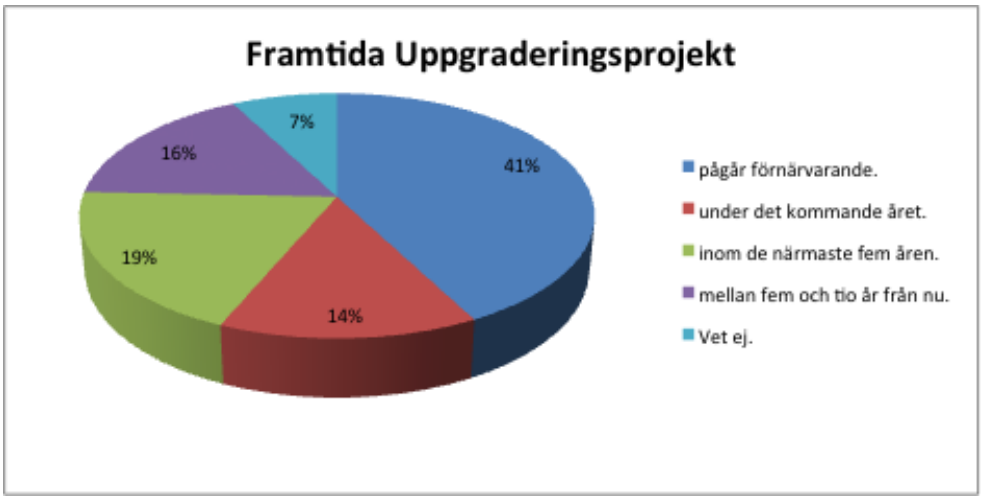
3.7 Resultat avsnitt F – Övriga aspekter

Det råder en stor skillnad vad beträffar hur organisationerna ser på systemuppgraderingar. I en del organisationer införs systemuppgraderingar omedelbart och hos vissa sker det inte alls:

- 20 % genomför omedelbara systemuppgraderingar
- 25 % genomför systemuppgraderingar vid behov
- 16 % genomför uppdateringar inom ett antal dagar (vilket i medeltal innebar 52 dagar för respondenterna av enkäten)
- 5 % genomför aldrig systemuppgraderingar
- 18 % vet inte

Leverantörsberoendet är stort. Cirka 42 % anser sig vara mycket beroende av externa parter (dvs. utanför den egna organisationen) för att uppdatera/modifiera SCADA-relaterade system och program. Sammantaget är hela 88 % av respondenterna beroende av externt anlitad expertis för att ex vis genomföra förändringar i programmeringen av styr- och kontrollsystem.

Merparten av respondenterna (41 %) uppgav att det förnärvarande pågick uppgraderingar av deras befintliga SCADA-system. Sammantaget svarade 75 % av respondenterna att de kommer uppgradera sina SCADA-system inom de närmaste fem åren, se Figur 3-11.



Figur 3-10. De flesta kommer att uppgradera sina SCADA-system inom de närmaste fem åren.

4 Sammanfattande iakttagelser

Kartläggningen har påvisat ett antal områden där det finns möjligheter till förbättringar hos dricksvattenförsörjningen. De väsentligaste iakttagelserna från kartläggningen kan i huvudsak summeras till följande områden:

1) Tekniska säkerhetsaspekter
   a) Bristande separation: Flera SCADA-system är fysiskt sammankopplade med kontorsnätverk vilket i kombination med andra identifierade brister i förlängningen kan medföra av IT-incidenter kan ge upphov till störningar i verksamheten.

   b) Bristande kontroll av system och nätverksstatus: Flertalet saknar tekniska system och processer för löpande kontroll och utvärdering av status hos datornätverk och brandväggar vilket kan göra det svårare att upptäcka incidenter i form av otillåtna kopplingar eller intrång i system.

2) Administrativa säkerhetsaspekter
   a) Avsaknad av interna riktlinjer: Flera organisationer saknar en informationssäkerhetspolicy som tar hänsyn till SCADA-system.

   b) Bristande dokumentation: Många organisationer har en ofullständig process för att kontinuerligt kartlägga och sammanställa systemberoenden.

   c) Bristande riskanalyser: Många organisationer genomför ofullständiga riskanalyser, då dessa inte vare sig omfattar konsekvenser av havererade SCADA-system eller genomförs på korrekt dokumentationsunderlag (se ovanstående punkt).

   d) Otillfredsställande utbildning i informationssäkerhet: Flera organisationer anser att medvetenheten om vikten av informationssäkerhetsarbetet är eftersatt framförallt p.g.a. bristande förståelse och utbildning inom området.

   e) Bristfällig process för hantering av behörigheter: Flera organisationer brister när det gäller att byta ut leverantörs lösenord i system och nätverksutrustning samt behörigheterna för personal som slutar sin anställning.

   f) Otillfredsställande incidenthantering: Flera har dålig uppföljning av incidenter och bristande bevakning av potentiella säkerhetsproblem.

3) Övriga aspekter
    a) Bristande utvärdering av SCADA-säkerhet: Flera organisationer saknar rutiner för att regelbundet genomföra utvärderingar av informationssäkerheten hos SCADA-systemen och dess organisation.

    b) Bristfälliga upphandlingar: Flertalet organisationer saknar relevanta säkerhetskrav vid upphandling av system och tjänster. Vissa respondenter, där uppgraderingsprojekt pågår eller planeras, påpekar att även upphandlingskonsulter saknar relevant kunskap inom området SCADA-säkerhet.

    c) Bristande kontroll av externa parter: Merparten av respondenterna är mycket beroende av kunskapen och säkerhetsarbetet hos externa parter och underleverantörer. Trots detta genomförs sällan någon oberoende kontroll och uppföljning av dessa aktörer. Se (RPSFS 2010).

    d) Bristande utbildning i informationssäkerhet. Det finns behov av både säkerhetsrelaterad utbildning, ökad medvetenhet om SCADA-säkerhetens betydelse samt tydligare riktlinjer och checklistor för både VA-aktörer samt deras systemintegratörer/leverantörer.

5 Fortsatt arbete

5.1 Behov av fortsatt arbete

Författaren anser att resultaten från kartläggningen visar på behovet av förbättringsarbeten inom ett antal olika områden. Nedan ges exempel på två områden där fortsatt arbete är möjligt och viktigt.

5.2 Utbildning och medvetandehöjning

En ökad kompetens krävs på alla nivåer, både hos ledande chefer och hos driftteknikerutei processen. Dessa målgrupper kräver dock delvis olika typer av kursinnehåll.

En del underlag för kompetenshöjande insatser finns redan idag framtagna hos FOI. Med aktivt stöd från MSB har där dels utvecklats en tvådagars kurs om säkerhet i kontrollsystem (SIK) och dels har en mobil demonstrationsanläggning tagits fram för att möjliggöra utbildningar på plats hos enskilda organisationer.

För att nå ut bredare inom vattenbranschen kan även medvetandegörande insatser bestå av enklare seminarier och pedagogiska artiklar i branschtidningar. Det medvetandehöjande SCADA-säkerhetsseminarium som Svenskt Vatten, Livsmedelsverket och MSB anordnade i april 2010 gav ett stort antal uppslag till samarbeten och andra möjliga seminarier. Detta arbete bör därför följas upp.

5.3 Checklistor och riktlinjer

Underlaget från enkäten kan utgöra ett stöd för att utarbeta checklistor för en ökad SCADA-säkerhet inom dricksvatten-försörjningen.

Checklistorna kan vara av olika slag och täcka alltifrån risk och sårbarhetsanalys, kravhantering, upphandling, avtal och uppföljning m.m. Dessa kan med fördel även relatera till aktuella föreskrifter och standarder på området, se (ISO/IEC 2005; SLV 2008; MSB 2009; RPS 2010).

Befintliga råd och riktlinjer bör även ses över och anpassas utifrån den verklighetsbild som tagits fram via denna kartläggning.

Referenser

ANSI (2004). *Integrating Electronic Security into the Manufacturing and Control Systems Environment,* rapport ANSI/ISA-TR99.00.02-2004, utgiven av American National Standards Institute (ANSI).

Cegrell, T. & Sandberg, U. (1994). *Industriella styrsystem*. Borås: SIFU förlag.

CORE (2008). *CitectSCADA ODBC service vulnerability*, Core Security Technologies – CoreLabs Advisory [Elektronisk] Tillgänglig: <http://www.coresecurity.com/content/citect-scada-odbc-service-vulnerability>

CPNI (2009), *Good practice guidelines*, The Centre for the Protection of National Infrastructure (CPNI), England. [Elektronisk] Tillgänglig: http://www.cpni.gov.uk/Products/guidelines.aspx

ISO/IEC (2005a). ISO/IEC 27001:2005, Information Technology – Security Techniques – Information Security Management Systems – Requirements.

ISO/IEC (2005b). ISO/IEC 27002:2005, Information Technology – Security Techniques – Code of Practice for Information Security Management.

Johansson, E. (2005). *Assessment of Enterprise Information Security - How to make it Credible and Efficient*, Diss. Avdelningen för industriella informations- och styrsystem vid skolan för Elektro- och Systemteknik, Kungliga Tekniska högskolan (KTH), Stockholm, 2005.

Johansson E., et al. (2007). *Aspekter på antagonistiska hot mot SCADA-system i samhällsviktiga verksamheter*, Krisberedskapsmyndigheten (KBM), 2007.

Johansson, E. et al. (2009). Increasing the Security Awareness in the Water Sector is a Choice of Color - Will you take the blue pill or the red pill?, *American Water Works Association (AWWA) Water Security Congress,* Washington DC, USA, 8-11 April 2009.

Johansson, E. et al. (2009). Practical Security Assessment of SCADA-systems - Experiences from a drinking water facility, *American Water Works Association (AWWA) Annual Conference and Exposition (ACE)*, San Diego, USA, 14-18 Juni 2009.

KBM (2006). *Basnivå för Informationssäkerhet (BITS) 2006:1*, rapport utgiven av Krisberedskapsmyndigheten (idag Myndigheten för samhällsskydd och beredskap, MSB).

KBM (2008). *Vägledning till ökad säkerhet i digitala kontrollsystem i samhällsviktiga verksamheter,* utgiven av Krisberedskapsmyndigheten, författad av Åke J Holmgren, Erik Johansson och Robert Malmgren.

MSB (2007). *Forum för informationsdelning avseende informationssäkerhet – SCADA och processkontrollsystem (FIDI-SC),* Myndigheten för samhällsskydd och beredskap. [Elektronisk] Tillgänglig: <http://www2.msb.se/publikationsservice/>KBM / Broschyrer och faktablad / forum_info-delning_kring-sakerhet_SCADA-system.pdf.

MSB (2009a). *Vägledning till ökad säkerhet i industriella kontrollsystem*, utgiven av Myndigheten för samhällsskydd och beredskap, författad av Åke J Holmgren, Erik Johansson samt Robert Malmgren.

MSB (2009b). *MSBFS 2009:10 föreskrifter och allmänna råd om statliga myndigheters informationssäkerhet.* Myndigheten för samhällsskydd och beredskap. Tillgänglig: http://www.msb.se/RS/2009/MSBFS_2009-10.pdf

NICC (2008). *SCADA Security Good Practices for Drinking Water Sector.* Dutch National CyberCrime Infrastructure (NICC). Tillgänglig: http://www.samentegencybercrime.nl/

NIST (2007). *DRAFT Guide to Industrial Control Systems (ICS) Security.* Special Publication 800-82, National Institute of Standards and Technology (NIST), Gaithersburg. Tillgänglig: http://csrc.nist.gov/publications/PubsDrafts.html

RPSFS (2010). *Rikspolisstyrelsens föreskrifter och allmänna råd om säkerhetsskydd; beslutad den 17 december 2009 med stöd av 43 och 44 §§ säkerhetsskyddsförordningen (1996:633).* Rikspolisstyrelsens författningssamling. Tillgänglig: http://www.polisen.se/Global/www%20och%20Intrapolis/FAP/FAP244_1_RPSFS2010_3.pdf

SLV (2003). *Handledning för ökad IT–säkerhet inom dricksvattenområdet,* utgiven av Statens Livsmedelsverket (SLV) som rapport 4-2003.

SLV (2007). *Säkerhetshandbok för dricksvattenproducenter*, utgiven av Statens Livsmedelsverket (SLV) och Svenskt Vatten (SV).

SV (2009). svenskt Vattens hemsida (Elektronisk) Tillgänglig: <http://www.svensktvatten.se/web/Sakerhet_i_IT-system.aspx>

SVU (2009), *Projekt 29-120 Nulägesanalys av och förslag till åtgärder för ökad SCADA-säkerhet inom kommunal dricksvattenförsörjning.* Svenskt Vatten Utveckling. (Elektronisk) Tillgänglig: <http://www.svensktvatten.se/web/Pagaende_SVU-projekt.aspx>

Bilagor

Bilaga 1. Följebrev

Bilaga 2. Enkät

Svenskt Vatten
Swedish Water & Wastewater Association

Myndigheten för samhällsskydd och beredskap

Datum
2009-03-30

Beteckning
SCADA enkät

Svenskt Vattens medlemmar
VA-chef/VA-ansvarig/Säkerhetsansvarig

Inventering av digitala kontrollsystem (SCADA-system[1])

Introduktion

Bifogat detta brev finner ni en unik enkät, som är starten på Svenskt Vattens projekt om SCADA-säkerhet inom kommunal dricksvattenförsörjning. Enkäten handlar om informationssäkerheten i digitala kontrollsystem för dricksvatten. Enkäten är initierad och framtagen av Svenskt Vattens nybildade arbetsgrupp för ökad SCADA-säkerhet inom dricksvattensektorn (SV-SCADA) med stöd av Myndigheten för Samhällsskydd och Beredskap (MSB). Mer information om MSB, som stöder projektet ekonomiskt och med kunskap, finns på myndighetens hemsida: www.msbmyndigheten.se.

Syfte & mål

Enkäten, som troligen är den första i sitt slag, syftar till att kartlägga det aktuella informationssäkerhetsarbetet relaterat till digitala kontrollsystem (SCADA-system) inom kommunal dricksvattenförsörjning. Dessutom vill vi påvisa praxis, med andra ord vilka metoder som används inom branschen. Förhoppningsvis kan den insamlade informationen bidra till att sätta fokus på områden där vi behöver förbättra oss. För Svenskt Vatten är det oerhört betydelsefullt att få medlemmarnas syn och återkoppling inom ett område som blir allt viktigare.

Genomförande

Svaren i enkäten kommer att behandlas konfidentiellt. Analys och rapportering kommer inte att kunna spåras till någon individuell organisation.

Att fylla i enkäten är ett relativt omfattande arbete. Vi önskar att ni snarast avsätter tid och resurser så att ni på bästa möjliga sätt kan besvara frågorna. Besvara gärna enkäten tillsammans i en mindre grupp som exempelvis består av både ”SCADA-användare” och någon som är insatt i den lokala IT-infrastrukturen. Risken är annars att enkäten inte ger en korrekt helhetsbild över den lokala IT-säkerheten.

Besvarad enkät skickas per post i bifogat svarskuvert innan onsdagen den 6 maj 2009. Om svarskuvertet har försvunnit går det bra att skicka den direkt till följande adress: ”SCADA-enkät”, Svenskt Vatten, Box 47607, 117 94 Stockholm.

[1] Internationellt används vanligen SCADA-system (Supervisory Control And Data Acquisition) som en samlingsterm för *alla* former av digitala kontrollsystem, vilka även benämns processkontrollsystem, industriella informations- och styrsystem, process-IT, distribuerade kontrollsystem (DCS), inbyggda realtidssystem (RTE), tekniska IT-system samt t ex Programmable Logic Controllers (PLC).

Svenskt Vatten
Box 47607
SE-117 94 Stockholm
Sweden

BESÖK/VISITORS
Liljeholmsvägen 28
Stockholm

PHONE
+46-(0)8 506 002 00
FAX
+46-(0)8 506 002 10

E-MAIL
svensktvatten@svensktvatten.se
INTERNET
www.svensktvatten.se

VAT NO
SE556473-5248-01

Om ni har några praktiska frågor gällande enkäten kan ni kontakta Andreas Wiberg (070-862 2784) eller SCADA-säkerhetsspecialist Erik Johansson (070-686 1133).

Bakgrund

Säkerhet i samband med produktion och distribution av samhällets viktigaste livsmedel – dricksvatten – är naturligtvis av yttersta vikt. Då produktion och distribution av dricksvatten alltmer förlitar sig på datorbaserade styrsystem blir det därför allt viktigare att även dessa system fungerar säkert. Tyvärr kan ofta dessa IT-baserade system manipuleras på en rad olika sätt, vilket därmed kan utgöra en säkerhetsrisk. Att vidmakthålla säkerheten hos de processnära datorbaserade styrsystemen (vilka i bifogad enkät benämns med samlingstermen SCADA-system) är därför mycket viktigt. Störningar i dessa system kan inte bara avbryta kritiska funktioner (t.ex. avbryta desinfektionen), utan även leda till att dyrbar utrustning (såsom pumpar och ventiler) tar skada och måste bytas ut! Alla dessa IT-relaterade störningar kan i förlängningen leda till att kvaliteten på dricksvattnet påverkas. Förtroendet för dricksvattenförsörjningen kan komma att ifrågasättas av allmänheten, vilket är en annan möjlig allvarlig konsekvens.

Trots att de IT-relaterade säkerhetsriskerna med SCADA-system ökar befarar vi att medvetenheten bland våra medlemmar fortfarande är relativt låg kring hur allvarliga konsekvenserna i praktiken är för respektive verksamhet. De praktiska erfarenheterna och kompetens kring sårbarheterna i verksamheternas SCADA-system är idag alltför bristfällig, inte bara hos Svenskt Vattens medlemmar, utan dessvärre även hos de konsultbolag och leverantörer som anlitas vid exempelvis systemupphandlingar.

För att ändra på detta har Svenskt Vatten för avsikt att arbeta proaktivt med en långsiktig handlingsplan för att höja SCADA-säkerheten inom kommunal dricksvattenförsörjning. Det är vår förhoppning att Svenskt Vatten, genom den nystartade arbetsgruppen, kan bidra till en positiv utveckling inom SCADA-säkerhetsområdet, bland annat via kunskapsspridning, kompetensförsörjning, intressebevakning, kommunikation och samverkan.

Denna enkät avser som sagt att belysa praxis samt inventera både installerade system och våra medlemmars förmåga att hantera framtida utmaningar som hot och sårbarheter för med sig. Enkäten som bifogas baseras på såväl nationella som internationella erfarenheter om sårbarheter i SCADA-system, samt belyser en rad aktiviteter som kanske bör finnas på plats för att säkerställa IT-säkerheten hos produktions- och distributionsanläggningar för kommunalt dricksvatten.

Tillsammans har vi ett stort ansvar att skydda våra anläggningar och vår personal mot de framtida hotbilder som vi idag knappt känner till. Se till att ge branschen en klar bild över sina styrkor och svagheter genom att frågorna i enkäten blir besvarande på bästa sätt. Vi emotser er enkät inom ca fyra veckor, dvs månadsskiftet april/maj.

Stockholm mars 2009

Lena Söderberg	*Andreas Wiberg*	*Erik Johansson*
VD Svenskt Vatten	*Svenskt Vatten*	*Tekn. Dr. KTH*

Utvalda referenser och informationskällor

Johansson, E., Malmgren, R., J.Holmgren, Å. (2008) *Increasing the security awareness in the water sector is a choice of color - Will you take the blue pill or the red pill?* Antagen till konferensen AWWA 2009 Water Security Congress.

Johansson, E., et al. (2008) *Practical Security Assessment of SCADA-systems - Experiences from a drinking water facility,* Antagen till AWWA ACE 2009.

Holmgren, Å., Johansson, E., Malmgren, R. (2008) *Vägledning till ökad säkerhet i digitala kontrollsystem i samhällsviktiga verksamheter.* Forum för informationsdelning avseende informationssäkerhet – SCADA och processkontrollsystem (FIDI-SC), Krisberedskapsmyndigheten.

Johansson, E. Et al. (2008) *Security Issues for SCADA Systems within Power Distribution*, Nordic Distribution and Asset Management Conference.

Johansson, E., et al. (2007) *Aspekter på antagonistiska hot mot SCADA-system i samhällsviktiga verksamheter*. Krisberedskapsmyndigheten.

Johansson, E. (2005) *Assessment of Enterprise Information Security - How to make it Credible and Efficient,* Doktorsavhandling vid KTH.

Shaw, W. T. (2006) *Cybersecurity for SCADA systems*. PennWell Corp., Tulsa.

NIST SP 800-82 – Guide to Industrial Control Systems (ICS) Security, National Institute for Standards and Technology (NIST), U.S.

Det pågår ett omfattande internationellt arbete kring säkerhet i digitala kontrollsystem. Ett bra sätt att hålla sig uppdaterad är att regelbundet följa vad som skrivs på några av de etablerade webbsidorna. Följande sidor är en bra start:

Centre for the Protection of National Infrastructure (CPNI), U.K.
www.cpni.gov.uk/ProtectingYourAssets/scada.aspx

Dep. of Homeland Security, US-CERT, Control Systems Security Program, U.S.
www.us-cert.gov/control_systems/

American Water Works Association
www.awwa.org/

INVENTERING AV DIGITALA KONTROLLSYSTEM (SCADA-SYSTEM)

Denna enkät är framtagen av Svenskt Vattens nybildade arbetsgrupp för ökad SCADA-säkerhet inom kommunal dricksvattenförsörjning (SV-SCADA) med ett finansiellt stöd av Myndigheten för Samhällsskydd och Beredskap (MSB). Syftet är dels att kartlägga informationssäkerhetsarbetet relaterat till digitala kontrollsystem samt dels att påvisa praxis inom branschen, dvs. vilka metoder/processer som används, samt identifiera eventuella förbättringsområden.

Alla svar kommer att behandlas konfidentiellt! All sammanställning, analys och rapportering kommer att ske anonymiserat och kommer inte spåras till någon individuell organisation.

OBS! Er ifyllda enkät måste hanteras förtroligt då den kan komma att innehålla känsliga uppgifter!
Skicka ifylld enkät direkt till följande adress:
"SCADA-enkät", Svenskt Vatten, Box 47607, 117 94 Stockholm.

Instruktioner:

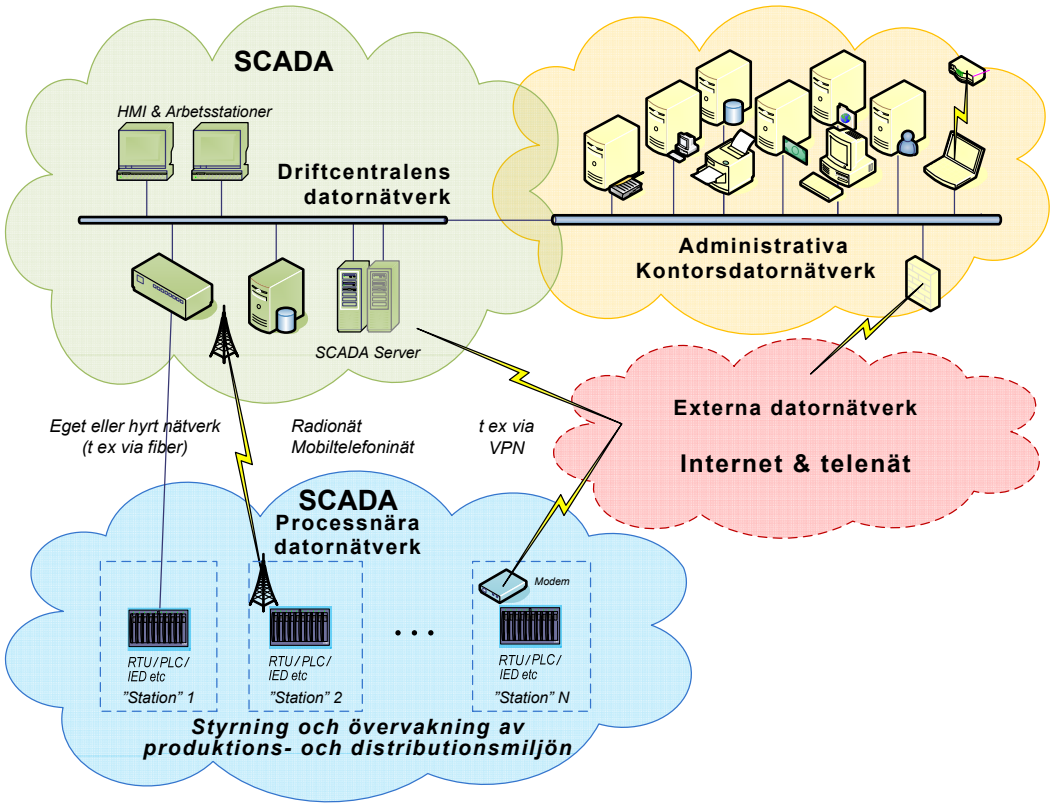
1) Välj svar genom att sätta ett kryss, för det alternativ som bäst överensstämmer med era förhållanden.
2) Enkäten innehåller även ett antal personliga frågeställningar för att fastställa kompetensprofilen i VA branschen.
3) Den engelska termen SCADA (Supervisory Control and Data Acquisition) används i denna enkät som ett samlingsbegrepp för all form av processkontroll styrning som kan tänkas användas inom vattensektorn.

Vid ev. frågor gällande enkäten vänligen kontakta Andreas Wiberg (070-862 2784) eller Erik Johansson (070-686 1133).

A. REFERENSMODELL

Nedanstående referensmodell (se figur 1) syftar till att förtydliga delar av den terminologi som används i de efterföljande frågorna. I denna referensmodell skiljer vi framförallt på följande fyra områden:

- driftcentralens datornätverk, (grönfärgade molnet),
- processnära datornätverk, (blåfärgade molnet),
- administrativa kontorsdatornätverk, (gulfärgade molnet), samt
- externa datornätverk, (rödfärgade molnet).



Figur 1. Referensmodell för att förtydliga terminologin som använts i denna enkät. Notera att termen SCADA används som ett samlingsbegrepp för all form av processkontrollstyrning som återfinns såväl i driftcentralens datornätverk (gröna molnet) som i produktions- och distributionsmiljön (blå molnet). Övriga områden som ofta interagerar med SCADA-system är datorsystem i det administrativa kontorsnätverket (gula molnet) samt datorsystem från underleverantörers tjänster som befinner sig på externa nätverk utanför er kontroll (röda molnet).

B. BAKGRUNDSINFORMATION

1) Kapacitet
Vad är er totala produktionskapacitet (m^3 dricksvatten per dag)?

2) Storlek
Hur många personer/kunder är beroende av er vattenproduktion/distribution?

3) Befattning
Vilken är din/er[1] nuvarande befattning/roll i organisationen?

4) Erfarenhet
Hur många år har du/ni[1] haft denna befattning?

5) Bakgrund
Vilken är din/er[1] bakgrund (tidigare befattningar inom VA-området, utbildning etc.)?

6) Åldersprofil
För att bedöma åldersprofilen i branschen frågar vi efter din/er[1] ålder? Ange gärna även födelseår.

- ☐ UNG – yngre än 35 år,
- ☐ MEDEL – mellan 35 och 50 år,
- ☐ MOGEN – mellan 50 och 60 år,
- ☐ ERFAREN – över 60 år.
- ☐ Födelseår: .....

7) Aktuell kompetens inom er organisation
Anser du/ni att det inom er organisation idag saknas viss kompetens för att på bästa sätt kravställa, utveckla, underhålla, vidmakthålla och höja informationssäkerheten i era SCADA-system?

- ☐ Nej, all nödvändig kompetens finns inom den egna organisationen.
- ☐ Nej, nödvändig kompetens erhålls idag alltid genom våra externt anlitade underleverantörer.
- ☐ Ja, inom vår organisation saknar vi framförallt kompetens inom följande områden:

.....

.....

.....

8) Framtida stöd inom området
Anser du att Svenskt Vatten framöver bör erbjuda sina medlemmar ett ökat stöd inom SCADA-säkerhetsområdet?

- ☐ Nej, vi har själva all kompetens som behövs.
- ☐ Nej, vi anlitar extern kompetens om så behövs.
- ☐ Ja, vi skulle vara betjänta av stöd och råd inom följande områden (prioritera gärna 1-5, där 1 är viktigast):
  - o råd & riktlinjer för kravställande vid upphandling
  - o råd & riktlinjer för hur egen praktisk utvärdering av SCADA-system kan genomföras
  - o kompetenshöjande insatser som utbildningar och seminarier
  - o förmedla kompetens om nya hot och risker samt identifierade sårbarheter
  - o förmedla förvärvad erfarenhet vid upphandlingar och underhåll
  - o bearbeta leverantörerna i branschen så att dessa ökar sina insatser för ökad SCADA säkerhet
  - o annat (ange vad):

.....

.....

.....

.....

[1] *Om möjligt ser vi gärna att ni lämnar information om alla individer som bidrar med att lämna uppgifter i enkäten. Ni kan med fördel komplettera dessa svar på enkätens sista sidor där det finns utrymme för extra information.*

C. TEKNISKA ASPEKTER

9) Sammanställning över systemberoenden

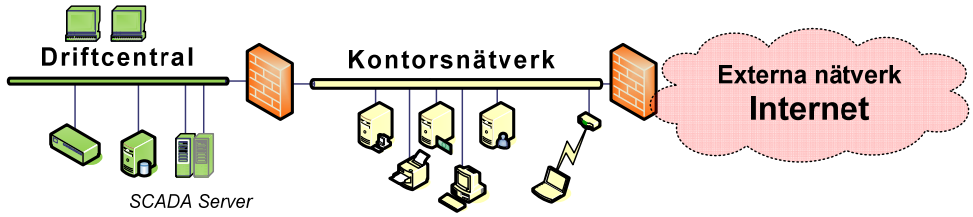
Finns det en komplett uppdaterad sammanställning (t ex i form av nätverksdiagram eller liknande) över SCADA-systemets alla delsystem och komponenter samt deras kopplingar/beroenden till andra IT-system och nätverk? (se ex vis figur 1).

- ☐ Ja, det finns en sådan sammanställning.
- ☐ Ja, men den befintliga avser enbart SCADA-systemet.
- ☐ Nej, den som fanns är inte längre uppdaterad.
- ☐ Nej, det finns inte någon sådan sammanställning.
- ☐ Vet ej.

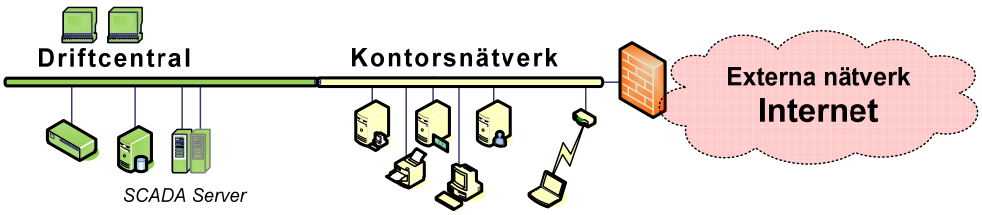
10) Nätverksarkitektur

Vilken av nedanstående figurer överensstämmer bäst med den lösning ni har för era datornätverk?
(om inget alternativ stämmer in, rita gärna en egen skiss vid bokstaven ”D”)

☐ A



☐ B



☐ C

☐ D

11) Regelbunden granskning

Utförs regelbundet utvärdering av vilka kopplingar som finns från SCADA-systemet till andra system?

- ☐ Ja, detta övervakas kontinuerligt.
- ☐ Ja, en regelbunden kontroll initieras manuellt.
- ☐ Nej.
- ☐ Vet ej.

12) Integration av SCADA

Finns det andra kopplingar eller datautbyten med SCADA-systemet utöver de egna kontorsnätverken?

- ☐ Ja.

  Om Ja, ange vilka: .....
  .....
- ☐ Nej.
- ☐ Vet ej.

13) Gränser för SCADA-system

Anser du att det finns en tydlig gräns mellan de system som ”tillhör” SCADA-system och de som inte gör det? Studera gärna referensmodellen, figur 1 i avsnitt A, på första sidan i enkäten.

- ☐ Ja.
- ☐ Nej.

14) Fysisk separation av SCADA-system

Är ert SCADA-system med dess nätverk **fysiskt** helt separerat från kontorsnätverk och Internet? Dvs. att utformningen av olika lokala nät (eller andra kommunikationssystem i nättopologin) är ”galvaniskt” isolerade från varandra.

- ☐ Ja.
- ☐ Nej.

  Om svaret är nej, varför inte? .....
  .....

15) Logisk separation av SCADA-system

Är ert SCADA-system med dess nätverk **logiskt** separerat från kontorsnätverk och Internet? Dvs nättopologin består av fysiskt samma infrastruktur men datorer kan ej kommunicera mellan de olika logiska nätverken.

- ☐ Ja.

  Hur är den logiska separation utförd? .....
  .....

- ☐ Nej. Om svaret är nej, fortsätt med fråga 17.

16) Kontroll av separation

Genomförs kontroller (ex vis regelbunden revision/inspektion) för att säkerställa att separationen mellan SCADA-system och kontorsnätverken vidmakthålls?

- ☐ Ja.

  Av vem? .....
  Hur ofta? .....

- ☐ Nej.

17) Styra och övervaka avlägsna platser

Används SCADA för att styra och övervaka avlägsna platser i produktions- och distributionsmiljön?

- ☐ Ja.
- ☐ Nej. Om svaret är nej, fortsätt med fråga 20.
- ☐ Vet ej

18) Kommunikationsteknologier för fjärrstyrning

Hur sker kommunikationen med avlägsna platser (ex vis pumpstationer)? (flera alternativ kan vara möjliga).

- ☐ eget datornätverk (t ex fibernätverk)
- ☐ hyrt datornätverk (t ex fibernätverk)
- ☐ telenät (t ex ISDN, modem)
- ☐ radiokommunikation (t ex mikrovågor, GSM, GPRS)
- ☐ internet (t ex VPN tunnel)
- ☐ Annat (ange gärna vad): .....

19) Utökad säkerhet i kommunikationslänkar

Använder ni utökade säkerhetsåtgärder för att skydda dessa kommunikationslänkar?

- ☐ Ja.

  Vilken typ? .....

- ☐ Nej.

20) Inkoppling av utrustning

Tillåter ni att extern underhållspersonal kopplar in (ex vis en bärbar dator) till ert SCADA system/nätverk?

- ☐ Ja.
- ☐ Nej – Hur säkerställs detta? .....
  .....

21) Tillåten fjärrstyrning

Tillåter ni fjärrstyrning av utrustning för

- ☐ Egen felsöknings/underhållspersonal.
- ☐ Underhåll från leverantör/integratör av system för dricksvattenprocessen.
- ☐ Felsökning från leverantör/integratör av system för dricksvattenprocessen.
- ☐ Ingen fjärrstyrning är tillåten.

  Hur säkerställs detta? .....

22) Elektronisk behörighetskontroll

Finns det vid elektroniska accesspunkter mekanismer för att kontrollera åtkomsten (t ex lösenordsskydd eller kontroll av nätverksadress)?

- ☐ Ja, på alla.
- ☐ Ja, på vissa.

  Om Ja, ange hur detta sker: .....
  .....

- ☐ Nej.

23) Djupledsförsvar

Finns ett försvar i djupled (defence-in-depth), dvs används flera nivåer av skydd och överlappande säkerhetsmekanismer, för att skydda SCADA-system och dess delkomponenter?

- ☐ Ja.
  - Om Ja, ange hur detta sker: .....
    .....
    .....
- ☐ Nej.
- ☐ Vet ej.

24) Härdning av system

Har SCADA-systemet och dess delkomponenter ”härdats”, dvs att alla oanvända tjänster och dataportar avaktiveras?

- ☐ Ja, alla delar.
- ☐ Ja, vissa delar.
- ☐ Nej.

25) Standardlösenord

Finns det standardlösenord (s.k. ”defaultlösenord” som är generiska) vilka ger tillgång till system/utrustning?

- ☐ Ja.
- ☐ Nej.
- ☐ Vet ej.

26) Antivirusskydd

Finns antivirusskydd installerat på datorer?

I kontorsdatornätverket:	Ja [ ]	Nej [ ]	Vet ej [ ]
I driftcentralens datornätverk:	Ja [ ]	Nej [ ]	Vet ej [ ]
I processnära datornätverk & utrustning:	Ja [ ]	Nej [ ]	Vet ej [ ]

27) Fysiskt skydd

Finns fysiskt skalskydd (t ex staket och låsta dörrar) som omgärdar SCADA-system och dess komponenter?

- ☐ Ja, både för kontrollrummet (driftcentralen) och andra känsliga lokaler (ex vis pumpstationer).
- ☐ Ja, men bara för kontrollrummet (driftcentralen).
- ☐ Ja, men bara för känsliga lokaler (ex vis pumpstationer).
- ☐ Nej.

28) Fysisk behörighetskontroll

Finns det vid dessa fysiska accesspunkter kontinuerlig övervakning (t ex med kamera och/eller inbrottslarm)?

- ☐ Ja, för både kontrollrummet och stationer.
- ☐ Ja, för kontrollrummet.
- ☐ Ja, för stationer.
- ☐ Nej.

29) Övervakning och kontroll av fysiskt skydd

Finns det vid fysiska accesspunkter kontinuerlig övervakning (t ex med kamera och/eller inbrottslarm) och kontroll av det fysiska skyddet?

- ☐ Ja, alla fysiska accesspunkter övervakas och det fysiska skyddet utvärderas löpande.
- ☐ Ja, för kontrollrummet (driftcentralen).
- ☐ Ja, för andra känsliga lokaler (ex vis pumpstationer).
- ☐ Nej.

30) Dataflöden

Vilka informationsflöden finns in och ut från driftcentralens datornätverk (markera med kryss)?

Typ av data	Data flödar **in** i SCADA-systemet	Data flödar **ut** ur SCADA-systemet
Mätdata, vattenflöden samt tryck i distributionsnätet		
Mätdata, fyllnadsnivåer i reservoarer		
Underhållsdata (t ex arbetsordrar)		
GIS (dvs geografisk informationsdata)		
Kunddata		
Data till kontorsapplikationer		
Säkerhetskopiering av data		
Annat (ange vad):		

D. ORGANISATORISKA ASPEKTER

31) Tydliga roller och ansvar

Finns det hos er en tydlig roll- och ansvarsfördelning för informationssäkerhetsarbetet?

- ☐ Ja.
- ☐ Nej. Om nej, varför inte? .....
- ☐ Vet ej.

32) Ansvarig för informationssäkerheten i SCADA-system

Finns det hos er en specifik person utsedd som ansvarar för allt informationssäkerhetsarbete relaterat till SCADA-system?

- ☐ Ja,
  Uppge namn & befattning: .....
  .....
- ☐ Nej. Om nej, varför inte? .....
- ☐ Vet ej.

33) Säkerhetspolicy för SCADA-system

Finns det en specifik informationssäkerhetspolicy för SCADA-systemet?

- ☐ Ja, ett eget dokument finns framtaget enbart för SCADA-system.
- ☐ Ja, SCADA-systemet omfattas av ett tillägg till den generella informationssäkerhetspolicyn.
- ☐ Nej.
- ☐ Vet ej.

34) Process för kartläggning och riskanalys

Finns det en specifik process för att löpande kartlägga och genomföra riskanalyser av era SCADA-system och nätverk?

- ☐ Ja.
- ☐ Nej. Om nej, varför inte? .....
- ☐ Vet ej.

35) Utbildning i informationssäkerhet

Har personal med tillgång till SCADA-system genomgått grundläggande informationssäkerhetsutbildning?

- ☐ Ja, samtliga (inklusive de som ”bara” har tillgång till de lokaler där SCADA-system utrustning finns).
- ☐ Ja, vissa nyckelpersoner.
  Om ja, ange typ av utbildning? .....
- ☐ Nej.
- ☐ Vet ej.

36) Individuella användarkonton

Finns kontroller som gör att enskilda datorkonton (administratörskonton och användarkonton) inte delas mellan flera användare/operatörer?

- ☐ Ja.
- ☐ Nej. Om nej, varför inte? .....
- ☐ Vet ej.

37) Policy för byten av lösenord

Hur ofta måste användare ändra sina lösenord?

- ☐ en gång var _____ - dag.
- ☐ på uppmaning av systemansvarig (t ex efter att en operatör byter jobb/slutar).
- ☐ Aldrig.

38) Byte av standardlösenord

Ändrar ni alla standardlösenord som finns inlagda av system- och infrastrukturleverantörer?

- ☐ Ja.
- ☐ Nej. Om nej, varför inte? .....
- ☐ Vet ej.

39) Bakgrundskontroller

Görs bakgrundskontroller (t ex i brottsregistret) på personal och entreprenörer som ges tillgång till SCADA-system eller tillgång till de lokaler där de finns?

- ☐ Ja, på alla.
- ☐ Ja, på vissa. På vilka grunder sker urvalet?.....
- ☐ Nej.

40) Upphandling

Inkluderas alltid informationssäkerhetsmässiga krav i upphandlingsprocessen för SCADA-system, datornätverk och för de tjänster som kontrakteras?

- ☐ Ja.
  Om Ja, vilka riktlinjer eller standarder baseras dessa på? (t ex ISO/IEC 270001, NIST SP 800-82, BITS el likn)
  .....
- ☐ Nej.
- ☐ Vet ej.

41) Förändringshantering

Finns en dokumenterad process för förändringshantering kopplat till SCADA-systemet vilken hanterar förändringar kopplade till hårdvara och mjukvara?

- ☐ Ja.
- ☐ Nej.
- ☐ Vet ej.

42) Kontinuerlig intrångsdetektering

Finns det verksamhetsprocesser (t ex regelbunden genomgång av loggar) eller automatiserade verktyg för att gå igenom försök att få access och identifiera intrångsförsök via elektroniska accesspunkter?

- ☐ Ja, på alla accesspunkter.
- ☐ Ja, på vissa accesspunkter.
- ☐ Nej.
- ☐ Vet ej.

43) Procedur för hantering av underhåll

Finns etablerade procedurer för utvärdering av *hur* förändring och underhåll av SCADA-systemet påverkar säkerheten? (t ex vid uppdateringar och installation av patchar)

- ☐ Ja.
- ☐ Nej.
- ☐ Vet ej.

44) Backuper

Finns backuper på konfigurationer och data som gör att systemet snabbt kan återställas till samma skick som tidigare?

- ☐ Ja.
- ☐ Nej.
- ☐ Vet ej.

45) Incidenthantering

Finns en incidenthanteringsplan som beskriver hur IT-relaterade incidenter (attacker) ska rapporteras och vem som ska göra vad?

- ☐ Ja.
- ☐ Nej.
- ☐ Vet ej

46) Återställningsplan

Finns en återställningsplan som beskriver hur systemet ska återställas efter en incident inträffat?

- ☐ Ja.
- ☐ Nej.
- ☐ Vet ej.

47) Kontinuitetsplaner

Finns det några kontinuitetsplaner för SCADA-miljön?

- ☐ Nej.
- ☐ Ja, ange nedan vilka typer av åtgärder som omfattas:

- ☐ Redundant konfiguration.
- ☐ En regelbunden fullt genomtestad plan för att flytta styr och övervakning till en reservplats.
- ☐ Säker backup av konfigurationsdata lagrad på en avsides belägen plats.
- ☐ Prioriterad ”kund” hos leverantören/tillverkaren vid händelse av en katastrof.
- ☐ Annat (ange gärna vad): .....

.....

.....

.....

48) Manuell drift

Är det möjlighet att köra vattenverket helt ”manuellt” (dvs helt utan stöd från några digitala kontrollsystem)?

- ☐ Ja.
- ☐ Nej.
- ☐ Vet ej.

49) Resursbehov

Finns det *några* i er organisation som manuellt *kan* hantera driften av såväl produktions- som distributionssystem utan någon form av stöd från digitala kontrollsystem?

- ☐ Ja.

  Om Ja, hur många individer? .....

  Hur många individer anser ni behövs per dygn för att kunna hantera driften manuellt?

  Vid normal drift: .....

  Vid störd drift: .....
- ☐ Nej, det finns inte dessa resurser.
- ☐ Vet ej.

E. HOT & RISK ASPEKTER

50) Hotbild

Allt oftare förekommer artiklar om sårbarheter och hot mot våra datorbaserade system. I nedanstående tabell vill vi att ni i tre steg anger era uppskattningar beträffande attacker mot era datornätverk (dvs molnen i referensmodellen, se figur 1).

A) Vilka av nedanstående hot tror ni att SCADA-system troligen kan komma att utsättas för framöver?
B) Gradera risken för att bli utsatt för något av dessa hot under de kommande tio åren (skala 1-10, där 1=låg 10=hög risk).
C) Har ni redan utsatt för någon av dessa attacker mot något av era datorrelaterade nätverk (dvs molnen i referensmodellen)?

Hot	A) Kan utgöra ett tänkbart hot för oss	B) Risken för att vi blir utsatta inom 10 år (skala 1-10)	C) Detta har redan inträffat hos oss
Oriktade attacker (t ex via vanliga datorvirus)			
Riktade attacker i utpressningssyfte			
Anställda som *medvetet* begår felaktigheter			
Anställda som *omedvetet* begår felaktigheter			
Före detta anställdas hämnd/illvilja			
Terrorism/vandalism med politiska motiv			
Annat (ange vad):			

51) Sårbarheter

Vilka anser du/ni är de topp-5 största riskfaktorerna/sårbarheterna när det gäller SCADA-system i vattensektorn?

1.

2.

3.

4.

5.

52) Riskanalys

Utgör era SCADA-system och nätverk en del av den regelbundna affärsmässiga riskanalys som organisationen genomför?

- ☐ Ja.
- ☐ Nej.
- ☐ Vet ej

53) Incidenter

Har ni haft några (informations-) säkerhetsincidenter i era SCADA system och nätverk under de senaste åren?

- ☐ Nej.
- ☐ Vet ej, dvs känner inte till att vi har haft några incidenter.
- ☐ Jag vill inte svara på den här frågan.
- ☐ Ja.

Om ja, ange nedan antalet identifierade incidenter samt indikera gärna det aktuella problemområdet/ena för dessa.

Antal incidenter under 2008 + 2009: ..... st av typ .....
Antal incidenter under 2007: ..... st av typ .....
Antal incidenter under 2006: ..... st av typ .....
Antal incidenter tidigare: ..... st av typ .....

F. ÖVRIGA ASPEKTER

54) Systemleverantörer

Vilken/vilka fabrikat av SCADA-system används hos er för att styra och övervaka dricksvattenprocessen?

- ☐ ABB modell: ..... installationsår:.....
- ☐ Cactus modell: ..... installationsår:.....
- ☐ Citect modell: ..... installationsår:.....
- ☐ FIX (GE/Fanuc) modell: ..... installationsår:.....
- ☐ Mitsubishi modell: ..... installationsår:.....
- ☐ SattControl modell: ..... installationsår:.....
- ☐ Siemens modell: ..... installationsår:.....
- ☐ Toshiba modell: ..... installationsår:.....
- ☐ VA-operatör modell: ..... installationsår:.....
- ☐ Andra viktiga leverantörer/integratörer av system/tjänster anlitar ni er av (relaterat till SCADA & IT-drift):

  ....

  ....

  ....

55) Antal systemleverantörer

Hur många olika systemleverantörer/integratörer använder ni er av (t ex för IT-drift, backup, modifieringar mm)?
För att bedöma eventuellt kritiska marknadsdominerande aktörer ser vi gärna att ni även anger namnen på de företag som är allra viktigast för att vidmakthålla er verksamhet:

56) Beroende av externa leverantörer

Hur beroende är ni av externa parter, dvs utanför den egna organisationen, för att uppdatera/modifiera SCADA-relaterade system och program?

- ☐ Mycket beroende, vi sköter själva den normala driften men alla modifieringar görs av kontrakterade externa systemintegratörer/leverantörer.
- ☐ Delvis beroende, vissa delsystem sköter vi helt själva men förändringar i programmeringar genomförs av externt anlitad expertis.
- ☐ Helt oberoende av externa resurser, vi sköter allting själva (modifieringar och underhåll av såväl hårdvara som programvara)
- ☐ Vet ej.

57) Systemuppgraderingar

Hur snabbt installeras uppgraderingar, s.k. ”patchar”, till SCADA-relaterade system och program?

- ☐ Omedelbart.
- ☐ Inom _____ dagar.
- ☐ Inom _____ veckor.
- ☐ Annat (ange vad): _____
- ☐ Aldrig.
- ☐ Vet ej.

58) Systemuppgraderingar

Har ni något specifikt handlingsprogram eller kvalitetsprocedur för att åtgärda kända säkerhetsproblem genom uppgraderingar av system?

- ☐ Ja.
- ☐ Nej.
- ☐ Vet ej.

59) Framtida uppgraderingsprojekt

När kommer ni att behöva uppgradera delar av ert befintliga SCADA-system?

- ☐ pågår förnärvarande.
- ☐ under det kommande året.
- ☐ inom de närmaste fem åren.
- ☐ mellan fem och tio år från nu.
- ☐ inte aktuellt, vi använder oss av befintliga system i mer än tio år till.
- ☐ Vet ej.

Svenskt Vatten

Enkät för inventering av digitala kontrollsystem (SCADA-system) *Ifylld enkät skickas till Svenskt Vatten.*

Ett stort TACK för er medverkan!

För att ge Svenskt Vatten möjlighet att återkomma med relevant information till er ser vi gärna att ni nedan lämnar era kontaktuppgifter.
Organisation:
Uppgiftslämnare:
Adress:
Telefon:
E-post:

Nedan kan Ni lämna egna synpunkter relaterade till SCADA-säkerhetsområdet för vatten sektorn. **Kom gärna med synpunkter på denna enkät. Vad saknades? Vad behöver förbättras? Vad behöver förklaras? Hur lång tid tog det att fylla i den? Hur många hos er engagerades?**

Nedan kan Ni lämna ytterligare information: