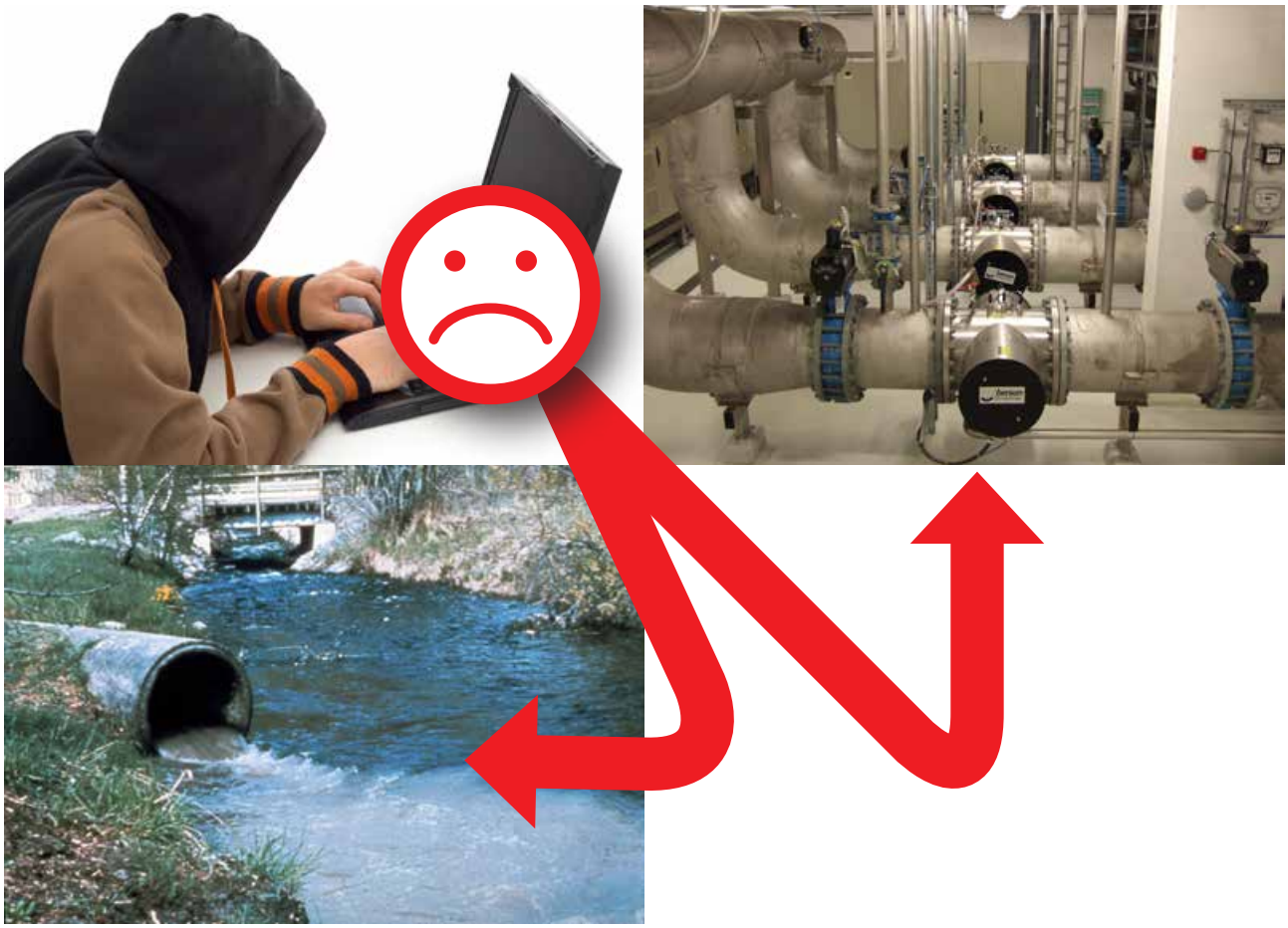
Norsk Vann

Rapport

195 | 2013

Sikkerhet og sårbarhet i driftskontrollsystemer for VA-anlegg



Norsk Vann

Norsk Vann Rapport

(Tidligere NORVAR-rapporter)

Det utgis 3 typer rapporter:

Rapportserie A:

Dette er de opprinnelige hovedrapportene. Dette kan være:

- Rapportering av prosjekter som er gjennomført innenfor organisasjonens eget prosjektsystem
- Rapportering av spleiselagsprosjekter hvor to eller flere andelseiere i Norsk Vann BA samarbeider for å løse felles utfordringer
- Rapportering av prosjekter som er gjennomført av andelseiere eller andre. Rapporten vil i slike tilfeller kunne være en ren kopi av originalrapporten eller noe bearbeidet

Fortløpende nummer xx-årstall

Rapportserie B:

Dette er en serie for «enklere» rapporter, for eksempel forprosjekter, som vil være grunnlag for videre prosjektvirksomhet mm.

Fortløpende nummer Bxx-årstall

Rapportserie C:

Dette er rapporter delfinansiert av Norsk Vann, men som er utgitt av andre.

Fortløpende nummer Cxx-årstall

Norsk Vann

Norsk Vann BA, Vangsvegen 143, 2321 Hamar
Tlf: 62 55 30 30 E-post: post@norskvann.no
www.norskvann.no

Forsidefoto: Christen Ræstad, Jozsef Szasz-Fabian og Arne Seim.

Norsk Vann Rapport

Norsk Vann BA

Adresse: Vangsvegen 143, 2321 Hamar
Telefon: 62 55 30 30
E-post: post@norskvann.no
Internettadresse: norskvann.no

Rapportnummer: 195 - 2013
ISBN 978-82-414-0340-8 ISSN 1504-9884 (trykt utgave) ISSN 1890-8802 (elektronisk utg.)
Dato: 11. mars 2013
Antall sider (inkl. bilag): 52
Tilgjengelighet: Åpen: x Begrenset:

Rapportens tittel:

Veiledning for sikkerhet av driftskontrollsystemer for VA-systemer

Forfatter(e):

Martin Gilje Jaatun
Jon Røstum
Stig Petersen

Ekstrakt:

Driftskontrollsystemer (DKS) som brukes til å styre og overvåke VA-systemene (vann-behandlingsanlegg, vanntransport, avløpstransport og avløpsrenseanlegg) er en viktig del av infrastrukturen knyttet til vann og avløp. Den stadig økende bruken av IKT innen drift av VA-systemer har gitt store muligheter for bedre overvåkning og styring, noe som har gitt samfunnet gevinster i form av økt effektivisering, pålitelighet og produktivitet, men har samtidig gjort VA-sektoren mer sårbar for nye typer trusler. DKS har gått fra å være lukkede systemer som bare virket på egne maskiner, til å bli integrerte systemer som også er tilknyttet kontorstøttesystemer og internett. Dette har introdusert nye farer og trusler. Det er kjent at IKT-baserte styringssystemer kan manipuleres på ulike måter, noe som medfører at systemene i seg selv kan utgjøre en sikkerhetsrisiko.

Veiledningen har som mål å peke på uønskede hendelser som kan oppstå i DKS og gi konkrete råd og anbefalinger til tiltak som kan gjøre DKS og bruken av disse enda sikrere. Anbefalingene er i første rekke rettet mot ansvarlige i de ulike VA-verk (ledelse og IT-ansvarlig), men vil også være nyttige for tilsynsmyndighet. Målet er at DKS skal bli sikrere og mer robuste slik at de klarer å motstå de fleste uønskede hendelser. Dersom en hendelse likevel skulle oppstå, skal det gå kort tid å få systemet opp å gå igjen. I veiledningen er det lagt vekt på å vise gode eksempler og gi gode råd på hvordan sikkerheten av driftskontrollsystemer kan forbedres. Det er utarbeidet enkle sjekklister for å identifisere mulige sårbarheter i VA-verkene knyttet til DKS.

Emneord, norske:	Emneord, engelske:
Informasjonssikkerhet, driftskontrollsystem, vann og avløp	Information security, SCADA, Water and wastewater systems

Forord

Vann- og avløpsanleggene i Norge representerer samfunnskritisk infrastruktur. De skal fungere døgnet og året rundt, overvåket og kontrollert av dyktige fagfolk.

I den grad det har funnet sted sabotasje mot de norske anleggene har dette, til nå, i stor grad vært fysisk sabotasje med innbrudd i høydebasseng, tagging av utestasjoner eller ødeleggelser av veibommer. Imidlertid blir anleggene mer og mer styrt av data- og informasjonssystemer, med fjernovervåking, kontroll og drift gjort fra eksterne datamaskiner og portable enheter. Dette krever at vann- og avløpsverkene ivaretar sikkerhetsnivået på en ny måte. Anleggene skal ikke bare sikres fysisk, det skal også være umulig for uvedkommende å logge seg inn og fjernstyre anleggene. Styring skal kun skje av autorisert personell med riktig adgang- og kontrollmuligheter.

Denne rapporten tar opp ulike sikkerhetsvurderinger som må gjøres for at kommuner og anleggseiere skal

- sikre vann- og avløpsanleggene mot sabotasje fra uautorisert personell
- sikre systemene mot menneskelige feil
- sikre anleggene mot uønskede hendelser
- sikre anleggene mot sårbarhet for elektromagnetisk puls og interferens

I et systematisk oppsett er rapporten en veiledning til særlige krav til sikkerhet og beredskap for driftskontrollsystemer, den kommer med anbefalinger om hvilket sikringsnivå anleggseier bør legge seg på og hvordan et helhetlig beredskapskonsept skal utformes.

Norsk Vann håper eierne av vann- og avløpsanlegg benytter rapporten aktivt i sitt arbeid med å sikre at uvedkommende ikke får adgang til den norske infrastrukturen.

Rapporten og prosjektet har vært finansiert gjennom Norsk Vanns prosjektsystem. Forfatter har vært Sintef ved Martin Gilje Jaatun, Jon Røstum og Stig Petersen.

Styringsgruppa har bestått av:
Johnny Sundbye, Movar
Harald Rishovd, Oslo kommune VAV
Elsa Storeng, Oslo kommune VAV
Ragnar Paulsen, TAU

Rapporten finnes digitalt på www.norskvann.no. Her ligger det også en sjekkliste som anleggseier kan benytte for å kvalitetssikre at det er tatt hensyn til ulike sikkerhetsaspekter rundt anleggene.

Norsk Vann retter en stor takk til forfatterne og alle som har bidratt med innspill og synspunkter underveis i utarbeidelsen av rapporten.

Hamar, 11. mars 2013
Ingrid Holøyen Skjærbakken

Innholdsfortegnelse

1 Innledning 8
1.1 Generelt om informasjonssikkerhet 9
1.2 Trusler mot IKT-systemer 10
2 Driftskontrollsystem og driftskontrollsikkerhet 11
2.1 Definisjoner 11
2.2 Bruk av driftskontrollsystem i VA-sektoren 11
2.2.1 Funksjonene til et driftskontrollsystem 13
2.2.2 Kommunikasjon med utestasjoner 14
2.3 Driftskontrollsystem og risiko 17
2.3.1 Driftskontrollsystem som en kritisk komponent innen VA 18
2.3.2 Drivere og trender som vil påvirke fremtidig DKS sikkerhet og mulighetene for å øke sikkerheten 19
2.4 Eksempler på historiske uønskede hendelser ved driftskontrollsystemer 20
2.5 Sikkerhetsloven og forskrift om skjermingsverdige objekter innen VA og konsekvenser for driftskontrollsystemer 22
3 Årsaker til svikt i driftskontrollsystem 24
3.1 Tilfeldige og utilsiktede feil 27
3.1.1 Teknisk svikt. 27
3.1.2 Naturgitt skade. 27
3.1.3 Menneskelige feil 27
3.2 Bevisst skadeverk 28
3.2.1 Generelle angrep 29
3.2.2 Målrettede angrep 29
4 Helhetlig beredskapskonsept for organisasjonen 30
4.1 Risiko og sårbarhetsanalyse 31
4.2 Mål om robuste VA-systemer 32
4.3 Hendelseshåndtering 33
4.3.1 Forberedelsesfasen 34
4.3.2 Deteksjons- og reparasjonsfasen 34
4.3.3 Læringsfasen 35
5 Tiltak for å redusere sårbarheten 36
5.1 Retningslinjer for informasjonssikkerhet knyttet til DKS 36
5.1.1 Virksomheten og DKS henger sammen 36
5.1.2 Organisatorisk IT-sikkerhet 36
5.1.3 Basis for sikkerhetspolitikken 37
5.1.4 Grunnleggende premiss for DKS sikkerhetspolitikk 37
5.1.5 Fysisk beskyttelse 38
5.1.6 Ansvar 38
5.1.7 DKS integrert i risikohåndtering 38
5.2 Sikkerhetsbevissthet 38
5.2.1 Bevissthetsprogram 38
5.3 Revisjon 38
5.3.1 Årlig revisjon 38
5.3.2 Ekstern revisjon 38
5.4 Anskaffelsespolitikk for driftskontrollsystemer og –tjenester 38
5.4.1 Opprettholdelse av drift 38
5.4.2 Minimumskrav 39
5.4.3 Drift & vedlikehold fra tredjepart 40
5.5 Tekniske sikringstiltak 40
5.5.1 Brannmur 41
5.5.2 Dybdeforsvar 41
5.5.3 Separat DKS og kontornettverk 42
5.5.4 Reell mulighet til å koble DKS fra kontornettverket 43
5.5.5 Sikre forbindelser til DKS-nettverk 43

5.5.6 Revisjon av forbindelser 43
5.5.7 Internett 43
5.5.8 Overføring via åpne nett 44
5.5.9 Fjernaksess fra åpne nett 44
5.5.10 Trådløse nett 45
5.5.11 Modem 45
5.5.12 Sikkerhetskomponenter 45
5.5.13 Sikre DKS og nettverkskomponenter 45
5.5.14 Dokumentasjon av konfigurasjon 45
5.5.15 Konfigurasjonskontroll 46
5.5.16 Antivirus 46
5.5.17 Oppdatering 46
5.5.18 Sikker beskyttelse av DKS-miljøet 46
5.5.19 Autorisert utstyr 47
5.5.20 Utstyr fra tredjeparter 47
5.5.21 Passordpolitikk for DKS 47
5.5.22 Personlige passord og kontroll med brukertilgang 48
5.5.23 Forretningskontinuitet for DKS og nettverkskomponenter 48
5.5.24 Sikkerhetskopiering 48
5.5.25 Lagring av sikkerhetskopi 49
5.5.26 Verifisering av sikkerhetskopier 49
5.5.27 Administrasjon av lagringsmedia i DKS-miljøet 49
5.5.28 Krav til strømforsyning til driftskontrollanlegg 49
5.5.29 Reparasjonsberedskap 49
5.6 Sjekkliste for sikre driftskontrollsystemer innen vann og avløp 50
6 Referanser 53

Sammendrag

Driftskontrollsystemer (DKS) som brukes til å styre og overvåke VA-systemene (vann-behandlingsanlegg, vanntransport, avløpstransport og avløpsrenseanlegg) er en viktig del av infrastrukturen knyttet til vann og avløp. Den stadig økende bruken av IKT innen drift av VA-systemer har gitt store muligheter for bedre overvåkning og styring. Økt bruk av DKS innen VA har muliggjort en effektivisering i form av reduserte kostnader og færre ansatte for å drifte de samme VA-anleggene. Videre kan man nå innføre bedre VA-tjenester som tilbyr raskere responstid ved hendelser og bedre overvåkning av anleggene. Økt brukt av IKT innen styring og overvåkning av VA-systemene har også gitt samfunnet gevinster i form av økt effektivisering, pålitelighet og produktivitet, men har samtidig gjort VA-sektoren mer sårbar for nye typer trusler. DKS har gått fra å være lukkede systemer som bare virket på egne maskiner, til å bli integrerte systemer som også er tilknyttet kontorstøttesystemer og internett. Det er kjent at IKT-baserte styringssystemer kan manipuleres på ulike måter, noe som medfører at systemene i seg selv kan utgjøre en sikkerhetsrisiko.

Veiledningen har som mål å peke på uønskede hendelser som kan oppstå i DKS og gi konkrete råd og anbefalinger til tiltak som kan gjøre DKS og bruken av disse enda sikrere. Anbefalingene er i første rekke rettet mot ansvarlige i de ulike VA-verk (ledelse og IT-ansvarlig), men vil også være nyttige for tilsynsmyndighet. Målet er at DKS skal bli sikrere og mer robuste slik at de klarer å motstå de fleste uønskede hendelser. Dersom en hendelse likevel skulle oppstå, skal det gå kort tid å få systemet opp å gå igjen. I veiledningen er det lagt vekt på å vise gode eksempler og gi gode råd på hvordan sikkerheten av driftskontrollsystemer kan forbedres. Det er utarbeidet enkle sjekklister for å identifisere mulige sårbarheten i VA-verkene knyttet til DKS.

English summary

This report is published in Norwegian by Norwegian Water BA (Norsk Vann BA).

Address:	Vangsvegen 143, NO-2321 Hamar, Norway
Phone:	+ 47 62 55 30 30
E-mail:	post@norskvann.no
Website:	www.norwegian-water.no / www.norskvann.no
Report no:	195 - 2013
Report title:	The aim for security systems in water and waste water infrastructure
Date of issue:	March 11th 2013
Number of pages:	52
Keywords:	Information security, SCADA, Water and wastewater systems
Author:	Martin Gilje Jaatun Jon Røstum Stig Petersen
ISBN:	978-82-414-0340-8
ISSN	1504-9884 (printed edition)
ISSN	1890-8802 (electronic edition)

Summary:

The industrial information and control systems (ICS) used to control and supervise water and wastewater systems (water treatment, water transport, wastewater transport and wastewater treatment facilities) is an important part of the water and wastewater infrastructure. The increasing use of ICT in management and operation of water and wastewater systems provides opportunities for improved supervision and control, and increased use of ICS in these systems enables improved efficiency, reduced costs, and reduced manpower requirements related to their daily operation. Furthermore, it is now possible to introduce improved water and wastewater services, offering reduced response time related to incidents, and improved supervision of the systems. While the increased use of ICT in the control of water and wastewater systems offers efficiency benefits, it also exposes the water sector to a new type of threats. ICS have evolved from being closed systems to fully integrated systems connected to office automation networks and even the internet. ICT-based control systems can be manipulated by malfeasors in various ways, and this implies that the systems themselves may pose a security risk.

This guide aims to identify undesired incidents that may occur in ICS, and to give concrete advice and recommendations for measures that can make ICS and their use more secure. The recommendations are primarily intended for management and IT administrators responsible for water and wastewater facilities, but will also be useful for regulatory authorities. The goal is for ICS to be more secure and robust, enabling them to prevent and withstand most unwanted incidents. If an incident nonetheless should occur, restoration of service shall be achieved with a minimum of delay. This guide emphasizes good examples and advice on how security of ICS can be improved. Simple checklists have been developed to facilitate identifying possible ICS vulnerabilities in facilities.

Definisjoner og forkortelser

BYOD	**"**Bring your own device". BYOD innebærer at ansatte tar med seg og bruker sin egen maskinvare, i form av smarttelefoner, bærbare datamaskiner og nettbrett, på arbeidsplassen
GPRS	General Packet Radio Service (tjeneste for datatrafikk i GSM-nettet)
DKS	Driftskontrollsystem
DoS	Denial of Service (tjenestenekt-angrep)
Herding	Konfigurasjon av et system slik at kun de komponenter (programvare og/eller maskinvare) som faktisk brukes er tilgjengelige, samt at alle tilgjengelige sikkerhetsmekanismer er tatt i bruk.
IKT	Informasjons- og KommunikasjonsTeknologi
Integritet	Det at informasjon og/eller utstyr ikke er endret av uvedkommende
Konfidensialitet	Det at informasjon ikke kan leses av uvedkommende
MTO	Menneske, Teknologi og Organisasjon
MTTR	Mean Time To Repair (gjennomsnittlig tid det tar å reparere/erstatte/-re-etablere en feilet komponent/system)
Nettbrett	Enkel datamaskin uten tastatur. Framstår i mange tilfeller som en forvokst smarttelefon.
NSM	Nasjonal sikkerhetsmyndighet (Norge)
ROS	Risiko Og Sårbarhet
SCADA	Supervisory Control And Data Acquisition
SLA	Service Level Agreement (avtale om kvalitetsnivå på leverte tjenester)
Smarttelefon	Telefon som har bruksmuligheter som en liten datamaskin. Kan også brukes til telefonsamtaler.
TNO	Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (Nederlansk forskningsinstitutt) http://www.tno.nl
Tilgjengelighet	Det at informasjon og/eller utstyr er tilgjengelig for autoriserte brukere når de har behov for det
VA	Vann og Avløp
VA-verk	VA-verkene er de ansvarlige for den virksomhet (privat, interkommunal eller kommunal) som produserer og leverer forsyningsvann til samfunnet (befolkning og industri) og som samler inn og renser avløpsvann fra samfunnet. Norsk Vanns medlemmer utgjør altså hoveddelen av denne aktørgruppen.

1 Innledning

Gode vann- og avløpstjenester er viktig for at samfunnet skal fungere. Folk trenger rent og trygt vann i tilstrekkelige mengder, og avløpsvannet må transporteres og behandles for å sikre miljøet og unngå at vannbårne sykdommer sprer seg. Det er viktig at vann- og avløpstjenestene er sikre og robuste. Vann og avløp er en kritisk infrastruktur; dersom disse tjenestene svikter vil det få store konsekvenser for samfunnet.

Driftskontrollsystemer (DKS) som brukes til å styre og overvåke VA-systemene (vann-behandlingsanlegg, vanntransport, avløpstransport og avløpsrenseanlegg) er en viktig del av denne kritiske infrastrukturen. Hendelser som medfører at et DKS ikke virker slik som forutsatt bør derfor identifiseres, og tiltak må settes inn både for å redusere risikoen for at dette skjer og for å redusere konsekvensene av slike hendelser.

Den stadig økende bruken av IKT innen drift av VA-systemer har gitt store muligheter for bedre overvåkning og styring. For eksempel kan i dag pumper og ventiler fjernstyres og overvåkes mye enklere enn tidligere. Større anlegg, slik som vannbehandlingsanlegg og avløpsrenseanlegg er også blitt mer kompliserte og krever avansert styring av de ulike integrerte prosessene. For de mest avanserte og komplekse vannbehandlingsanleggene spør man seg i dag om de i det hele tatt lar seg drifte uten at DKSene er i funksjon. Dersom svaret på dette er nei, vil det være svært viktig at DKSene virker til enhver tid og dette må gjenspeiles i de krav til tilgjengelighet og oppetid en setter for anlegget og dets støttefunksjoner.

Økt bruk av DKSer har muliggjort en effektivisering i form av reduserte kostnader og færre ansatte for å drifte VA-anleggene. Videre kan man nå innføre bedre VA-tjenester som tilbyr raskere responstid ved hendelser og bedre overvåkning av anleggene. Økt brukt av IKT innen styring og overvåkning av VA-systemene har også gitt samfunnet gevinster i form av økt effektivisering, pålitelighet og produktivitet, men har samtidig gjort VA-sektoren mer sårbar for nye typer trusler. DKSene har gått fra å være lukkede systemer som bare virket på egne maskiner, til å bli integrerte systemer som også er tilknyttet kontorstøttesystemer og internett. Dette har introdusert nye farer og trusler. Det er kjent at IKT-baserte styringsystemer kan manipuleres på ulike måter, noe som medfører at systemene i seg selv kan utgjøre en sikkerhetsrisiko.

God praksis for sikkerhet i drikkevannsektoren er dokumentert i en rapport fra det nederlandske forskningsinstituttet TNO [1]. Denne veiledningen bygger videre på denne, med tilpasninger for norske forhold. Vi har også skjelet til NVEs forslag til revidering av beredskapsforskriften for strømforsyning [2].

Veiledningen har som mål å peke på uønskede hendelser som kan oppstå i DKS og gi konkrete råd og anbefalinger til tiltak som kan gjøre DKS og bruken av disse enda sikrere. Anbefalingene er i første rekke rettet mot ansvarlige i de ulike VA-verk (ledelse og IT-ansvarlig), men vil også være nyttige for tilsynsmyndighet. Målet er at DKS skal bli sikrere og mer robuste slik at de klarer å motstå de fleste uønskede hendelser. Dersom en ulykke likevel skulle oppstå, skal det gå kort tid å få systemet opp å gå igjen.

1.1 Generelt om informasjonssikkerhet

Når det gjelder sikring av IKT-systemer og den informasjonen som ligger i disse systemene snakker man gjerne om sikring av[1]:

- **Konfidensialitet**; det å sikre at informasjonen er tilgjengelig bare for dem som har autorisert tilgang. Eksempel på tap av konfidensialitet er at hackere får tilgang til hemmelig informasjon som ligger lagret i driftskontrollsystemet (DKS).

- **Integritet;** det å sikre at informasjonen og metodene/beregningene er nøyaktige og fullstendige. Dette innebærer at uvedkommende ikke kan endre informasjonen eller systemet som behandler informasjonen. Eksempel på tap av integritet er at hackere logger seg på DKS til et vannbehandlingsanlegg og endrer kjemikaliedoseringen slik at det blir over- eller underdosering.

- **Tilgjengelighet**; det å sikre autoriserte brukeres tilgang til informasjon og tilhørende ressurser ved behov. Eksempel på tap av tilgjengelighet er at driftsoperatørene ikke klarer å logge seg på systemet og endre verdier ved behov.

I en utvidet definisjon av informasjonssikkerhet kan også følgende aspekter inkluderes:

- **Autentisering**; det å få visshet om at en part virkelig er den han/hun utgir seg for å være. Det gjelder både bruker og maskin (jfr. falske minibankautomater).

- **Ikke-benekting**; det å sikre at de som har sendt meldinger ikke kan benekte eller avvise det i etterkant.

- **Sporbarhet**; enhver endring av informasjon skal kunne spores; hvem som utførte endringen og når dette ble utført.

- **Personvern**; sikre at enkeltindividet kan kontrollere informasjon om en selv og hva denne brukes til. Alle har et behov for å være alene.

Når det gjelder drifts- og styringssystemer vil ofte integritet og tilgjengelighet være vel så viktig som konfidensialitet. Man er avhengig av at systemet er tilgjengelig og gjør de oppgavene det er satt til. Dette forutsetter også at systemet har tilgang til riktig informasjon til enhver tid.

Innføring av systemer som muliggjør fjernaksess innen drift av VA- systemer har gjort det enkelt og effektivt å få tilgang til status for VA-systemene utenom kontortid. Ved en hjemmevaktsordning kan operatør logge seg på anleggene og se på status på driften av anleggene og også utføre endringer i driftsbetingelse (slå av og på, lukke/åpne ventiler). Dette er en fordel sett ut i fra tilgjengelighet og effektivitet for brukerne. På den andre siden medfører muligheten for en slik ekstern pålogging til systemene en fare for at uvedkommende kan få tilgang til VA-systemene dersom ikke sikkerhetssystemene er gode nok. Dette kan således påvirke integriteten og til og med konfidensialiteten til systemet. Sårbarheter knyttet til bruk av IKT innen VA generelt, og DKS spesielt, er i mange tilfeller

[1] Definisjonene er hentet fra NS 7799:2003 Norsk standard for informasjonssikkerhet.

knyttet opp til avveininger mellom tilgjengelighet, integritet og konfidensialitet. Disse faktorene drar i forskjellig retning.

1.2 Trusler mot IKT-systemer

Trusler mot IKT-systemer er delt opp i to hovedkategorier:

- *Tilfeldige og utilsiktede feil* som kan skje på grunn av svakheter i IKT-systemet, uheldige ansatte eller utenforliggende hendelser.

- *Bevisst skadeverk* som igjen kan deles inn i:
  - *Generelle angrep* som ikke er direkte rettet mot VA-verket, men som kommer som en følge av det generelle trusselbildet mot IKT-systemer.
  - *Målrettede angrep* der angripere benytter IKT-systemer for å skade VA-verket spesielt.

Når man vurderer risikoen forbundet med truslene, må man også vurdere i hvilken grad mekanismer for å oppdage og håndtere hendelser eksisterer, og om disse tar for gitt at IKT, driftskontroll og samband fungerer. Det er også viktig å registrere historiske uønskede hendelser knyttet til IKT-systemene slik at en kan dra lærdom av disse hendelsene i etterkant og oppdatere eventuelle rutiner og prosedyrer. Disse truslene behandles i mer detalj i kapittel 3.

2 Driftskontrollsystem og driftskontrollsikkerhet

2.1 Definisjoner

Med driftskontrollsystem (DKS) menes prosess- og kontrollsystemer for overvåkning/ kontroll/styring av fysiske prosesser innen VA. Dette inkluderer styring av prosesser i vannbehandlingsanlegg og avløpsrenseanlegg, samt fjernkontrollsystemer for spredte geografiske anlegg for vanndistribusjon og avløpstransport. DKS inkluderer således det som på engelsk kalles:

- **Supervisory Control And Data Acquisition (SCADA)**. Brukes for å styre spredte geografiske anlegg som har behov for en sentral datainnsamling for felles styring av anleggene. Innen VA brukes SCADA typisk for distribusjon av drikkevann og innsamlingssystemer for avløpsvann. Ofte kalt fjernkontrollsystem.

- **Distributed Control Systems (DCS)**. Brukes for styring av lokale prosesser slik som for eksempel vannbehandlingsanlegg og avløpsanlegg.

- **Process Control Systems (PCS)** Kontroll og overvåkningssystemer som brukes for å påse at forskjellige prosesser opererer og opprettholdes innenfor optimale og sikre nivå.

- **Programmable Logic Controller (PLC)**/Programmerbar logisk styring (PLS) er styringsenhet som er tilkoblet utstyr direkte (ventiler etc.) for å automatisere oppgaver.

I denne veiledningen brukes begrepet driftskontrollsystem slik at det også inkluderer tilhørende støttesystemer som kommunikasjon og strømforsyning. Dette inkluderer fiberkabler, trådløs kommunikasjon, radio, fastlinje, GPRS, strømforsyning, utestasjoner, serverrom, PC, feltløsninger, brukergrensesnitt, driftskontroll sentral, programvare, back-up-system, web-basert tilgang, rapportsystem, sensorer og PLS'er i ute-stasjoner/målepunkter.

2.2 Bruk av driftskontrollsystem i VA-sektoren

I dette kapitlet beskrives vesentlige deler av IKT-systemene innen VA med fokus på drifts-kontrollsystemer.

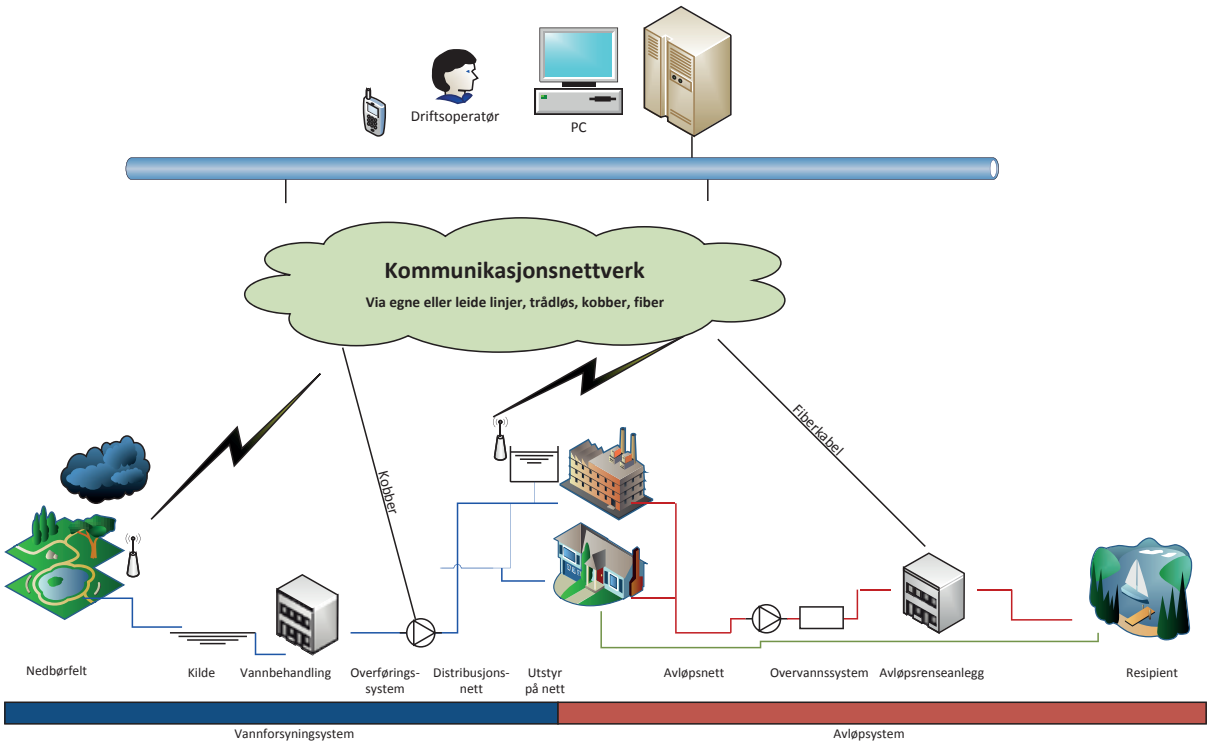
Figur 1 viser hele VA-kjeden fra nedbørfelt via vannbehandling og distribusjonsnett, til avløpsnett og videre til avløpsrenseanlegg og utslipp resipient (fjord, elv). Innenfor vann og avløp er det omfattende bruk av IKT- systemer knyttet til alle elementene i kjeden og ulike IKT-systemer benyttes for å styre og overvåke flere av disse prosessene. Dette inkluderer også ulike typer av systemer for samband og signaloverføring.

DKS består av ulike elektroniske komponenter som er plassert over et stort geografisk område. DKS varierer i oppbygging fra VA-verk til VA-verk, men består typisk av følgende komponenter: PC, DKS servere, terminaler for DKS (vaktsentral), nett, kabler (ethernet,

fiberkabler, kobberkabler), brytere, routere, IT-brannvegger, modem, telefonlinjer, radiosendere og mottakere, PLS'er, bærbare PC og smarttelefoner/mobiler.

Driftskontrollsystemet brukes for å styre vann og avløpssystemene, og for overvåking av ulike målepunkter både i nedbørfelt, på nettet og i prosessanlegg. Ulike utestasjoner er også koblet til driftskontrollsystemet; som vannpumpestasjoner, høydebasseng, reduksjonskummer, målekummer, avløpspumpestasjoner, påslippspunkter, avløp, overløp, nedbørstasjoner, vassdragsmålestasjoner og bekkerister. Prosessanlegg (vannbehandlingsanlegg og avløpsrenseanlegg) har ofte egne driftskontrollsystem som samler inn tilsvarende informasjon fra ulike målere/sensorer i disse anleggene. For en del VA-verk/kommuner har det historisk sett vært vanlig med ulike DKS for henholdsvis ledningsnett og prosessanlegg, kanskje med en eller annen form for overføring av måleverdier og alarmer mellom systemene.

Vann og avløpssektoren kjennetegnes av geografisk spredt infrastruktur. Særlig gjelder dette vann- og avløpsnettet som har anlegg og utestasjoner lokalisert der hvor behovet for anlegg er (kummer, pumpestasjoner osv). Tilhørende IKT- infrastruktur må følgelig være tilsvarende geografisk plassert. Dette er enklere for prosessanleggene slik som i vannbehandling og avløpsrensing hvor alt utstyr er samlet i en eller flere bygninger, noe som gjør fysisk sikring enklere.



*Figur 1: Vann og avløp fra nedbørfelt til resipient med angitt eksempler på hvordan driftskontrollsystem styrer og overvåker***.**

Hovedkomponentene i DKS kan deles inn i **menneske-maskin brukergrensesnitt** (HMI, Human Machine Interface), **sentralt system** og **lokalt system**. Driftsoperatøren styrer og overvåker VA-systemene via HMI som kan være PC'er på driftssentral, bærbar PC eller

aksess via web fra privat hjemme-PC. Hjernen i et driftskontrollsystem ligger i det sentrale systemet. Her samles data fra de ulike utestasjonene og det gjennomføres beregninger og prosessering av data. Det sentrale systemet må ha stor datalagringskapasitet for å lagre historiske data fra de ulike målepunktene. Basert på slike data kan trender i datamaterialet beregnes. Omfanget av det sentrale systemet vil variere avhengig av hvor omfattende og komplekst det enkelte VA-verk er. Lokalt system er typisk PLS montert i tilknytting til utstyr og prosess. Lokale system sørger for innsamling av data og lokal styring av enhet/utstyr. På lokalt nivå vil PLS'er kunne kommunisere med hverandre.

2.2.1 Funksjonene til et driftskontrollsystem

De viktigste funksjonene i et driftskontrollsystem er:

- **Datainnsamling** fra ulike målepunkter/sensorer. Dette inkluderer overføring av rådataverdier og omforming til måleverdier, prosessering av data som funksjon av tid, og kvalitetskontroll av de målte verdier. Driftskontrollsystemet er således et nyttig system for datainnsamling, og historiske data lagres for eventuell videre bearbeiding. Eksempler på data som samles inn kan være ventilstatus (åpen/lukket), data fra vannføringsmåler, UV-dose, turbiditetsmåler i vannbehandlingsanlegg og alarmverdier.

- **Overvåkning** av trender i dataserier med mulighet for angitte grenseverdier med tilhørende alarmfunksjoner når grensene overskrides. Driftskontrollsystemet har således en rolle både under daglig drift og i beredskapssituasjoner. Driftskontrollsystemet virker også som et alarmsystem hvor ulike typer alarmer er tilknyttet de enkelte utestasjoner. Alarmene er viktige for å kunne fange opp hendelser som er i ferd med å utvikle seg.

- **Styring/kontroll**. Alle utestasjoner hvor data skal logges har installert programmerbar logisk styreenhet (PLS). PLS kan styres lokalt (koble på med pc) eller via fjernstyring. Driften av anlegget kan endres sentralt fra driftskontrollsystemet (åpne/lukke ventiler, øke pådrag). Utestasjonene er ikke avhengig av kontakt med sentralt system eller kommunikasjon for å virke, men vil da styres ut fra grenser satt i lokal PLS. I tilfeller der man ikke får kontakt med utestasjonen, har man heller ingen kontroll med hva som skjer og kan ikke aktivt styre.

- **Planlegging og oppfølging**. De innsamlede data fra målestasjoner muliggjør systematiske analyser i ettertid for å følge opp driften av anlegget og se på trender. Dette kan f.eks. være analyse av pumpedata for å identifisere eventuelle økte lekkasjer på nettet eller endringer i forbruk.

- **Vedlikehold og systemendringer**. DKS muliggjør endring av driftsmodus, oppgradering av systemfunksjoner, og nyutvikling av funksjoner. Oppgraderinger og endringer i kritiske støttesystemer, slik som DKS, samtidig som vann og avløpstjenestene skal foregå som normalt, medfører at en har lite rom for feil.

2.2.2 Kommunikasjon med utestasjoner

Driftskontrollsystemet samler inn informasjon og data fra geografisk spredte anlegg (se Figur 1). Særlig gjelder dette for vann og avløpsnettet hvor det er ulike målepunkter spredt over større områder, men også inne i prosessanlegg er det viktig med sikker overføring av signaler fra målepunkt til datasenteret. Kommunikasjon kan foregå via fiberforbindelser, på vanlige kobberlinjer og via mobilnettet. Med slike løsninger skal man kunne nå alle stasjoner uansett hvor man er.

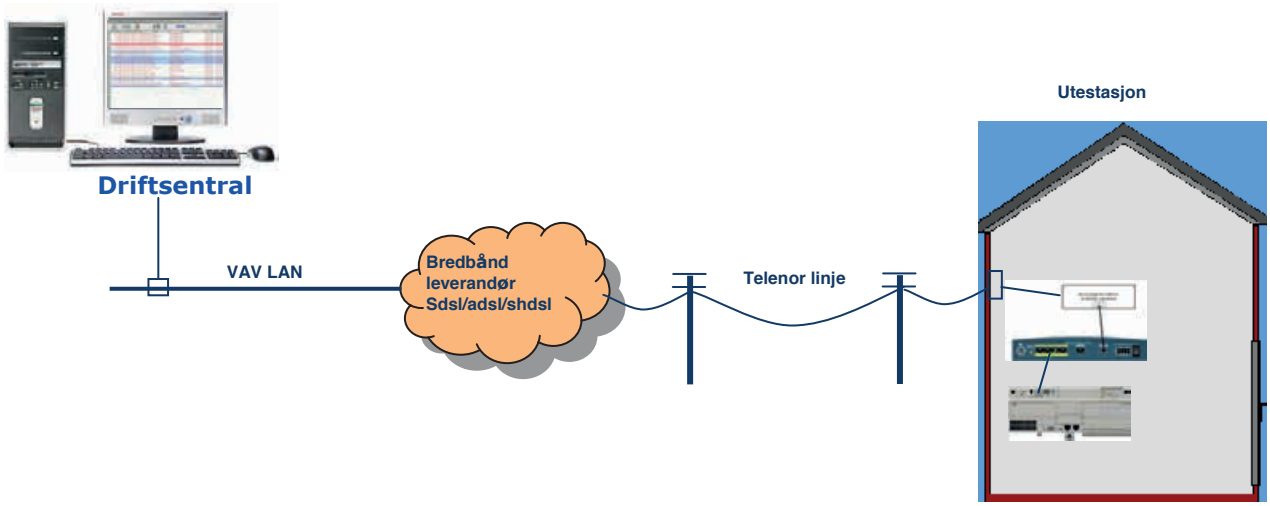
Ikke alle målepunkter/sensorer trenger å være tilknyttet driftskontrollsystemet. De utestasjonene som er valgt tilknyttet driftskontrollsystemet, er anlegg som er mer kritisk enn andre.

Driftskontroll utføres fra eventuelle vaktsentraler/beredskapssentre eller fra bærbare PC-er fra hjemmevakt. I det siste har også bruk av smarttelefoner for styring og overvåkning blitt vanlig.

Smarttelefoner og nettbrett har mange fordeler slik som mindre vekt, rask oppstart, lett mobil tilkobling, integrert kamera/video, GPS, lang batteridrift og stort utvalg av applikasjoner (app'er), men har som regel dårligere innebyggede sikkerhetssystemer enn hva som er vanlig for PC. Dette gjør at VA-verket lettere kan bli eksponert for IT-angrep.

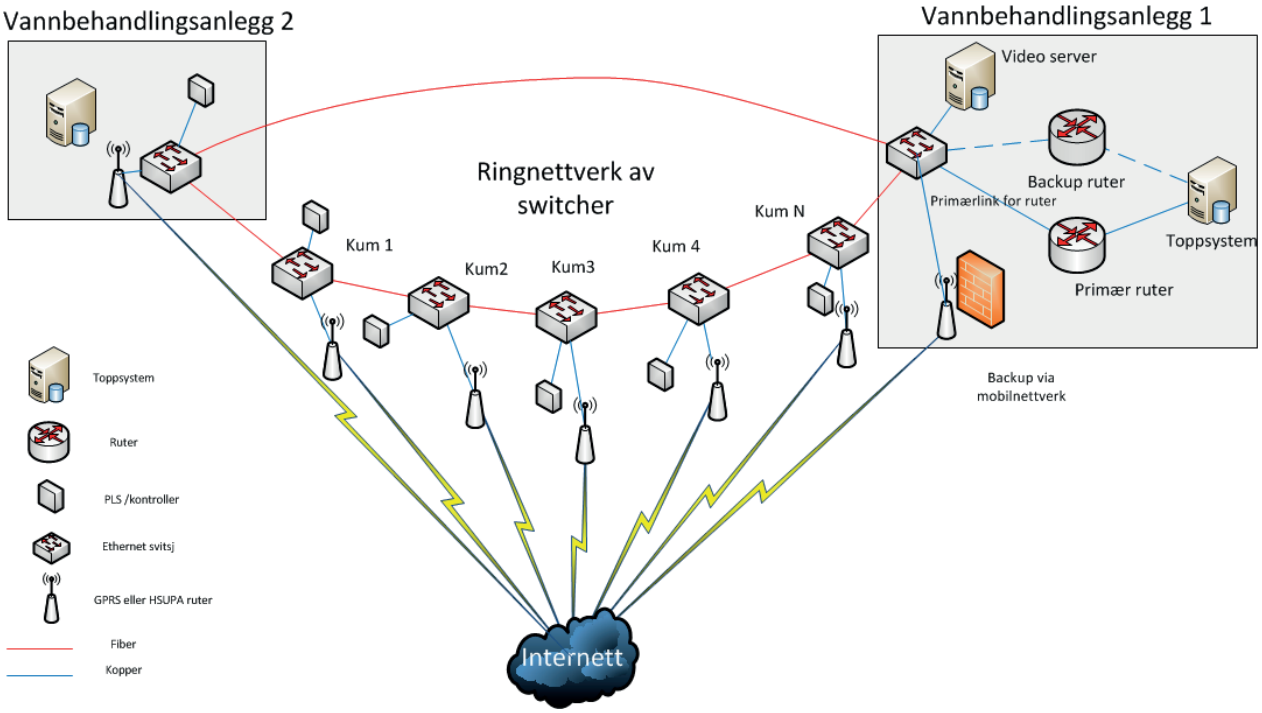
På PC er det ofte vanlig med sikkerhetsmekanismer i form av ekstra pålogging via et Virtuelt Privat Nettverk (VPN) eller "remote dekstop"-løsninger som Citrix. Bruk av smarttelefoner er enkelt og praktisk, og systemutviklerne ser teknologiske muligheter, men problemet vil være at en først ser de tekniske mulighetene og siden tenker på IT-sikkerheten. Ulike former for mobil administrasjon- og sikkerhetsløsninger, samt løsning for fjernstyring og overvåking av alle mobile enheter som brukes i virksomheten bør etableres. Man kan da overvåke uønskede applikasjoner, sørge for at sikkerhetsregler er på plass, utføre sletting av enheten dersom den kommer på avveie og enkelt kunne distribuere mobile applikasjoner og løsninger til de ansatte. Applikasjonsvirtualisering (f.eks. via Citrix) er en løsning som allerede finnes for nettbrett og enkelte smarttelefoner. En slik løsning vil sikre at applikasjoner for fjernaksess kun kan startes etter forutgående autentisering, og vil utgjøre et ekstra lag av sikkerhet mot ondartet kode på mobilt utstyr. Applikasjonsvirtualisering bør tas i bruk der hvor en gjennomgang av risiko og sårbarhet tilsier at dette er nødvendig.

Figur 2 og figur 3 viser typisk oppsett for kommunikasjon mellom utestasjoner og driftssentral. På Figur 2 er det angitt bare en kommunikasjonslinje fra utestasjon til driftssentral, men for anlegg som er særlig kritisk bør det være doble linjer (dvs. redundans) med hensyn til kommunikasjon og signaloverføring. En bør sikre ekte redundans i form av flere innføringspunkter i bygning og ulike typer av kommunikasjon (f.eks. GPRS) slik at en ikke har en falsk trygghet. For eksempel er det bredbåndsleverandører som bruker andre leverandører sitt kommunikasjonsnett og ikke har egen infrastruktur; ved svikt på kommunikasjonen hos hovedleverandør vil da også alternativ kommunikasjonsvei svikte. Trådløse systemer (GSM/GPRS/UMTS, radiolinje) er godt egnet som en backup til en kablet primær kommunikasjonslinje (fiber, bredbånd) for å oppnå full redundans.



Figur 2: Kommunikasjon mellom utestasjoner og driftssentral (figur fra Oslo VAV)

I senere år har det blitt vanlig å opererer med virtuelle servere, der en fysisk server kan framstå som flere forskjellige servere for brukerne. Her er det viktig å merke seg at dette i utgangspunktet ikke gir noen redundans i forhold til fysiske feil (hvis den fysiske serveren går ned, vil også alle de virtuelle serverne gjøre det). Med mer avanserte konfigurasjoner der man har en klynge med fysiske maskiner som tilbyr virtuelle servere vil man også kunne ha økt robusthet mot fysiske feil. Virtuelle servere vil også gjøre det mulig kun å tilby en tjeneste per server. Dette gir økt sikkerhet ettersom en angriper som får tilgang til en tjeneste ikke umiddelbart får tilgang til annen informasjon på serveren.



Figur 3: Eksempel på detaljert oppsett for kommunikasjon mellom driftssentral og utestasjoner (Figur fra Trondheim kommune, tegnet av Ontime Networks)

Oppringt samband

VA-verk som fortsatt benytter seg av oppringt samband ved utestasjoner kan være utsatt for eksterne angripere. Tradisjonelt har slike oppringte modem lite fokus på IT-sikkerhet, og har vært populære mål for oppringningsforsøk ved at det ringes opp tusenvis av telefonnummer for å lete etter nummer som har et modem tilknyttet. Ved bruk av oppringt samband, må dette konfigureres med tilbakeringing slik at det kun er et sett av predefinerte nummer som tillates å koble opp forbindelsen. Tilbakeringingen bør strengt tatt foretas av et annet fysisk modem enn det som mottar forespørselen, for å sikre at linjen er blitt koblet ned i mellomtiden.

Trådløs kommunikasjon

Trådløs kommunikasjon er ofte et kostnadseffektivt og fleksibelt alternativ til kablet kommunikasjon. Det er reduserte krav til tilgjengelig infrastruktur (ikke behov for kabling) og det er enkelt å installere. Ulempen er derimot at informasjon sendes som elektromagnetiske bølger, et medium som i prinsippet er tilgjengelig for alle som er innen rekkevidde av bølgene. På grunn av dette, må særskilte tiltak og mekanismer benyttes for å ivareta sikkerheten til all informasjon som sendes over trådløse nett. Kravene som stilles til trådløs kommunikasjon med utestasjoner omfatter [3]:

- **Tilgangskontroll** Nødvendig for å hindre uautorisert tilgang til nettverket. Legitime enheter i det trådløse nettverket må være i stand til å detektere og avvise meldinger fra ikke-autoriserte enheter.

- **Datakonfidensialitet** Kryptering bør benyttes for å hindre uønsket tilgang til informasjon som blir overført i det trådløse nettverket.

- **Dataautentisering** Mottakeren i et trådløst nettverk bør være i stand til å verifisere at informasjonen som er mottatt er legitim, og at den har sin opprinnelse fra riktig senderenhet. Dette hindrer at uvedkommende kan bryte seg inn i nettverket og spre falske meldinger.

- **Dataintegritet** Informasjon som er overført fra en legitim kilde kan bli modifisert eller korrumpert i overføringen. Angripere kan ved å generere interferens og støy, påføre bitfeil og pakkefeil i et trådløst nettverk. Mottakeren må være i stand til å verifisere at mottatt informasjon er komplett og korrekt, og at den ikke har blitt modifisert eller skadet i overføringen.

- **Dataferskhet** For overvåknings- og styringssystemer er det viktig at mottatt informasjon er fersk, dvs. at det ikke er gamle meldinger som mottas. Dette kan oppstå hvis en angriper avlytter nettverket for senere å sende kopier av eldre meldinger på nytt for å skape problemer og uønskede hendelser.

Trådløs kommunikasjon er utsatt for angrep av forskjellig art og opprinnelse, og ethvert trådløst system som benyttes til overvåkning eller styring av VA-infrastruktur må ha robuste sikkerhetsmekanismer. Angrep på trådløse systemer kan klassifiseres i en rekke kategorier:

- **Tilfeldig assosiering** Utilsiktet tilgang hvor fremmede enheter kopler seg til et trådløst nett uten å være klar over at det skjer.

- **Ondartet assosiering** Tilsiktet tilgang hvor en angriper klarer å bryte seg inn i et trådløst nettverk på grunn av manglende og utilstrekkelige sikkerhetsmekanismer. Slik tilgang åpner for at angriperen kan overvåke og stjele data, brukerinformasjon og passord, i tillegg til å initiere andre angrep.

- **Mann-i-midten angrep** Angriper tilriver seg tilgang til et trådløst nettverk ved ondartet assosiering og overvåker nettverkstrafikk og brukeraktivitet.

- **Tjenestenekt** Et trådløst nettverk settes ut av spill av angripere ved å sende store mengder falske meldinger for å redusere kapasiteten til nettverket, eller for å sette det helt ut av spill.

- **Interferens** Når to eller flere trådløse systemer, som opererer i samme frekvensområde, på samme sted og til samme tid, forstyrrer hverandres informasjonsutveksling. Dette gjelder i hovedsak systemer som opererer i ikke-lisensierte frekvensbånd hvor det er fritt frem for bruk av forskjellige trådløse løsninger.

- **Avlytting** Så lenge man er innenfor rekkevidde av et trådløst nettverk er det mulig å lytte etter meldinger som sendes. Hvis systemet har manglende sikkerhetsfunksjoner som for eksempel kryptering, vil avlytting kunne gi en angriper tilgang til sensitive og kritiske data som overføres.

- **Jamming** Dette er en spesiell utgave av tjenestenekt hvor en angriper oversvømmer frekvensbåndet til et trådløst nettverk med høyeffekts støy som korrumperer all form for meldingsutveksling mellom enheter i nettet.

I tillegg er det en mengde spesifikke angrep som er avhenger av hvilke protokoller som benyttes og som krever detaljert kunnskap om egenskaper til det trådløse nettverket.

2.3 Driftskontrollsystem og risiko

Det er et faktum at driftskontrollsystemer blir mer og mer integrert med tradisjonelle kontorstøttesystemer og tilkobling til internett. Driftskontrollsystemene er ikke lenger selvstendige systemer, men integrerte løsninger, noe som gjør at driftskontrollsystemene får de samme sårbarhetene som vanlige IT-systemer (virus og hacking).

Tradisjonelt har det ikke vært stort fokus på informasjonssikkerhet i prosesskontrollsystemer, verken i VA-sektoren eller i industrien for øvrig. Det er imidlertid ferske eksempler på hacking av VA-verk via driftskontrollsystemet (DKS) i USA[2] og automatiserte verktøy gjør det nå enkelt for hackere å lete opp kontrollenheter som er koblet til internett[3]. Det er også enkelt for uvedkommende å skaffe seg informasjon om kritiske deler av et DKS via internett. Default passord for enkelte systemer kan finnes via internett der manualer og videoer for hvordan de ulike DKS virker kan lastes ned. Dette gjør det

[2] http://www.theregister.co.uk/2011/11/18/second_water_utility_hack/
[3] http://www.wired.com/threatlevel/2012/01/10000-control-systems-online/

mulig for ikke-eksperter å tilegne seg kunnskap om eventuelle sårbarheter ved de enkelte DKS. En undersøkelse i regi av Svenskt Vatten [4] pekte også på lite fokus på informasjonssikkerhet knyttet til SCADA systemer. Dette gjaldt både svake IT- løsninger i selve SCADA systemet, men også lite fokus på IT- sikkerhet i VA-verket selv.

Vanlige ROS-analyser av VA-sektoren har oftest fokusert på prosesstekniske problemstillinger. Siden kunnskap om IKT-systemer som regel representerer et fremmed fagområde for VA-ingeniører, behandles IT-relaterte sårbarheter i liten grad i ROS-analyser for de enkelte VA-verk. Tilsynsmyndighetene (Mattilsyn og Fylkesmann) har også tradisjonelt hatt lite fokus på sårbarheten knyttet til IKT og driftskontrollsystem.

IKT-systemer blir stadig viktigere innen kritisk infrastruktur. Trenden er at slike systemer i større grad utvikles basert på hyllevare (f.eks. MS Windows) i stedet for rene spesiallagede systemer. Man ser også oftere at slike systemer kobles mot for eksempel administrasjonsnett, som igjen gjerne er koblet mot Internett. Den økende bruken av IKT, sammen med økt bruk av hyllevare og økt sammenkobling mot andre nett, gjør at sårbarheten når det gjelder IKT-trusler er større enn før.

Trusselvurderinger viser en økning i angrep mot samfunnskritiske IKT-system. Nasjonal sikkerhetsmyndighet (NSM) har gjennom flere år pekt på den økte trusselen mot prosesskontrollsystem – særlig innen olje- og gassektoren, men det er også pekt på vann og avløp. Av den grunn er det viktig at VA-verkene har stor oppmerksomhet på å beskytte driftskontrollsystemene.

2.3.1 Driftskontrollsystem som en kritisk komponent innen VA

DKS utgjør en viktig del av mange VA-systemer. I hvilken grad klarer VA-verket å opprettholde funksjonen og tjenestene dersom DKS faller ut? Ved svikt av en pumpestasjon eller noen få pumpestasjoner kan man utplassere driftsfolk som manuelt styrer og overvåker systemene, men dersom styringen av alle pumpestasjonene og høydebasseng faller ut er det spørsmål om vannverket har tilstrekkelige mannskaper for en slik manuell operasjon. For avanserte prosessanlegg som vannbehandlingsanlegg, vil det derimot kunne være vanskelig å drifte anlegget uten at DKS virker. DKS vil i et slikt tilfelle være en kritisk infrastruktur i seg selv.

Mange VA-verk er flinke til å gjennomføre beredskapsøvelser. Bortfall av DKS bør være et av flere scenarioer som inngår i VA-verkenes beredskapsøvelser. Svikt av DKS samtidig med at det oppstår andre hendelser, vil være et svært relevant og utfordrende scenario. Et mulig eksempel kan være svikt av DKS for styring av et avansert vannbehandlingsanlegg samtidig som råvannskvaliteten endrer raskt seg på grunn av store nedbørmengder. I slike situasjoner vil faren for mikrobiell forurensing av råvannet være høy og det vil være viktig at vannbehandlingsanlegget fjerner forurensing og desinfiserer vannet godt. Lærdommen fra slike beredskapsøvelser kan også brukes til å revidere beredskapsplanene knyttet til svikt av DKS.

2.3.2 Drivere og trender som vil påvirke fremtidig DKS sikkerhet og mulighetene for å øke sikkerheten

I det følgende beskrives en del drivere og trender som vil påvirke fremtidig sikkerhet for driftskontrollsystemer. Driverne er delt inn i henhold til administrative forhold, teknologiske forhold, VA-verkets behov og ønsker, og til slutt samfunnets behov.

Tabell 1. Drivere og trender som vil påvirke fremtidig DKS sikkerhet og mulighetene for å øke sikkerheten.

Administrativt	• Ønske om å koble sammen administrativt nett med nett for DKS for å effektivisere dataflyt (kostnadsbesparelser) • Effektivisering av driften ved å ha tilkobling til DKS også utenom vanlig arbeidstid (hjemmevakt) • Behov for ansatte med både god IT og VA-kompetanse • Problemer med å ansette nye folk med god kunnskap, mange erfarne som snart blir pensjonister • Avhengighet til leverandører og konsulenter og lite IT-kunnskap i egen organisasjon • Klimaendringer gir behov for mer styring og overvåkning • Økende krav og fokus fra tilsynsmyndigheter knyttet til IT sikkerhet • "Økt systemkontroll". Når DKS blir en del av IT sin leveranse eller ansvar, kreves tilgang for å føre kontroll med systemet. IT tar da deler av ansvaret fra DKS-leverandøren.
Teknologisk	• Raske teknologiske endringer og muligheter innen DKS (smarttelefoner, nettbrett). Leverandører er ofte raskt på banen med nye tekniske løsninger uten at en alltid har tenkt nok på sikkerhetsaspekter • Store endringer og vekst mht. trusler og uønskede hendelser knyttet til DKS. • Økende bruk av ikke-proprietær programvare. Dette medfører at leverandører av DKS går fra å ha et totalansvar for DKS, til å bli mer ansvarlig for integrasjon av sitt produkt inn mot andre systemer. Dette medfører også økte krav til kompetanse hos VA-verket (bestiller-kompetanse, totaloversikt) • Økende bruk av måleteknikk/sensorer og tilhørende kommunikasjonsbehov • Stadig mer komplekse anlegg/prosessanlegg som ikke kan driftes uten DKS
Driftsmessige hensyn	• Økt behov for raskere respons • Økt behov for styring og overvåkning av hele VA • Ønske om økt tilgjengelighet til IT-systemene 24 timer i døgnet, 7 dager i uken (24/7) blant ansatte • Økt behov for målepunkter innen VA som en følge av økte krav fra tilsynsmyndigheter, internkontroll, sanntidsstyring av systemene
Samfunnets behov	• Opprettholde samfunnets tillitt til at VA-verket leverer gode og sikre tjenester • Økt krav til service i befolkningen med raske responstider medfører økt behov for IKT • Høyere krav til sikkerhet i samfunnet som en følge av samfunnsutviklingen • Økt fare for IT- angrep mot samfunnskritiske funksjoner (nasjonalt og internasjonalt)

2.4 Eksempler på historiske uønskede hendelser ved driftskontroll-systemer

Figur 4 og Tabell 2 gir en kort gjennomgang av historiske uønskede hendelser (nasjonale og internasjonale) knyttet til svikt DKS med tilhørende støttesystemer (kommunikasjon, strøm).

CYBER-TOPPEN

Stuxnet fikk TU til å erklære «Cyberkrigen er i gang» i 2010. Sannheten er at krigsleken hadde vart ei stund allerede.

GLIMT FRA MODERNE CYBERKRIGSHISTORIE

1982: Stuxnets oldefar:
Sprengkraften i å manipulere industrielle styringssystemer har vært kjent i hysj-miljøet i 30 år. I 1982 greide CIA ved hjelp av noen linjer plantet datakode å overbelaste og videre sprenge i lufta en russisk gassledning i Sibir. Sovjet lå bak USA innen software-utvikling, og planla tyveri av flere industrisystemer. CIA valgte heller å sabotere enn å stanse tyveriet. Gasseksplosjonen utgjorde ca. en kvart Hiroshima-bombe og er blant de største ikke-kjernefysiske detoneringene i historien. Aksjonen ble først kjent 14 år senere.

1998: Radar-hack 1:
USA hacker seg inn i Serbias luftforsvarssystemer og setter serbiske flygeledere ut av spill. Trekket gjorde bombingen av serbiske mål lettere for USA og Nato under Kosovokrigen. Taktikken var så effektiv at en opprinnelig plan om å eskalere angrepet ble lagt til side fordi man fryktet det ville gå for hardt ut over sivile mål.

1998-2000: «Moonlight Maze»:
En systematisk tapping av informasjonssystemer fra Pentagon, Nasa, Energidepartementet, private universiteter og ulike forskningsinstitusjoner hadde pågått nesten to år da det ble oppdaget i 2000. Kilder har opplyst at inntrengerne skaffet seg opplysninger om kart over militære installasjoner, troppeforflytninger og militært utstyrsdesign. Angrepet ble sporet til servere i det tidligere Sovjet, men hendelsen er underlagt strengt hemmelighold og etterforskes den dag i dag.

2001: «Code Red»:
En dataorm i mange varianter fra juli 2001, som infiserte over 300 000 maskiner i USA. Det krevde felles innsats fra myndighetene og USAs nettleverandører for å hindre ormen fra å gjøre stor skade. Nettsteder som gikk ned, fikk påskriften «Hacked by Chinese».

2003-2004: Operasjon «Titan Rain»:
Koordinerte angrep på offentlige og private datasentraler i USA, trolig med forsvars/industrispionasje som hensikt. Lockheed Martin, Sandia National Laboratories (hvor hovedtyngden av USAs atomvåpen blir designet) og Redstone Arsenal (huser blant annet fly- og missilkommandoen) var blant dem som ble rammet. Lokalisert fra Kina, i ettertid antatt å ha militært utspring.

2007: Radar-hack 2:
Dypt inne i Syrias luftrom greide israelske F-15 og F-16-jagere 6. september 2007 å bombe en militærinstallasjon som antas å ha hatt en rolle i et samarbeidsprosjekt om atomteknologi mellom Syria og Nord-Korea. De israelske flyene kom seg helskinnet fram til målet takket være en målrettet hackeraksjon som satte Syrias luftforsvar og radarsystemer ut av spill til akkurat riktig tid. Israel og Syria har formelt vært i krig siden 1967.

1982
I 1982 greide CIA ved hjelp av noen linjer plantet datakode å overbelaste og videre sprenge i lufta en russisk gassledning i Sibir.

2007: Cyberangrepet på Estland:
Populært kalt «Web War I». En estisk/russisk krangel om rivingen av russiske krigsminnemerker i Tallinn utløste et massivt tjenestenektangrep som nær fikk all nettbasert informasjon i Estland til å stoppe opp. Parlamentet, departementene, sentrale banker, aviser og tv-kanaler ble rammet. Som i «alle» slike angrep, har opphavsmennenes formelle tilknytning til en stat (her: Russland) vanskelig latt seg bevise.

2008: Centcom-angrepet:
Ble ikke anerkjent av Pentagon før 2010. Tilsynelatende ubrukte minnepinner ble plassert i et vaskerom på en amerikansk militærbase i Midtøsten, i den tro at noen ville la seg friste. Det virket. Resultatet var at en dataorm penetrerte dypt inn i systemene til US military central command (Centcom). Opprydningen tok 14 måneder, og Russland sto igjen som hovedmistenkt.

2008: Georgia-angrepet:
Midt under konflikten mellom Georgia og Russland i august 2008, ble nasjonale medier og statlige nettsider utsatt for et massivt tjenestenektangrep med avsenderadresse Russland. Offentlige informasjonskanaler ble hindret i omtrent én uke, akkurat mens russiske troppeforflytninger var på sitt mest sårbare. Det ble som vanlig ikke funnet noen offisielle, formelle bånd mellom angriperne og en konkret nasjonalstat.

2009: GhostNet-angrepet:
Oppdaget i mars 2009 etter 10 måneders granskning fra kanadiske Information Warfare Monitor. Spionprogramvare koordinert fra kinesiske servere samlet informasjon fra interne offentlige datasystemer i hele 103 land. Ambassader, utenriksdepartementer og andre offentlige etater ble særlig rammet. Et tidlig fokus på eksiltibetanske miljøer styrket mistanken mot Kina.

2009: Operasjon Aurora:
Også kjent som Google-Kina-konflikten. I et av tidenes mest sofistikerte og koordinerte angrep greide kinesiske cyberangripere å hacke gmail-kontoer til kinesiske dissidenter og samtidig stjele interninformasjon fra it-tungvektere som Adobe, Yahoo! og Symantec, foruten Google selv. Angrepet førte til en opprivende konflikt mellom Google og kinesiske myndigheter, og diplomatiske problemer på statsnivå.

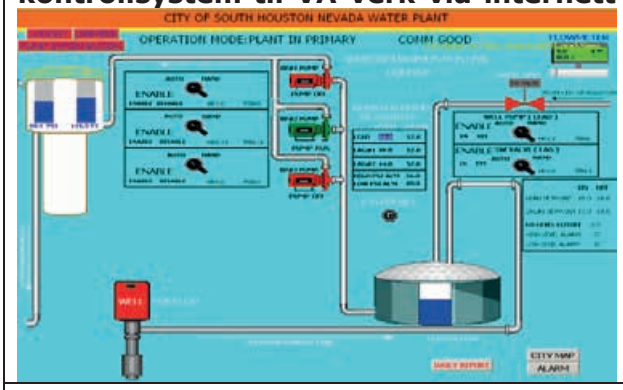
2010: Stuxnet:
Den globale cyberparanoiaens definitive gjennombrudd, og viruset som gjorde dataangrep anerkjent som en høyst virkelig og fysisk krigføringsmetode. Dataormen hadde sabotasje av urananrikingssentrifuger i iranske Natanz som mål. Sjonglerer mellom flere kategorier av svært sofistikert softwarehacking og storstilt, forutgående industrispionasje mot blant andre Siemens og driverprodusentene JMicron og Realtek. Å oppdage én såkalt «zero-day»-sårbarhet regnes som hard hackervaluta. Stuxnet hadde funnet og brukt smått uhørte fire slike sårbarheter i Windows-plattformen i ett og samme angrep. Regnet som det definitive høydepunktet innen malware. Antatt avsender: Israel/USA. Er programmert til å ødelegge seg selv om tre uker, 24. juni.

2011:«Shady RAT»-operasjonen:
Ifølge oppdageren McAfee en «pågående og målrettet operasjon utført av én spesifikk aktør» fra midten av 2006. Navnet spiller ikke bare på ordet rotte, men på akronymet RAT (Remote Access Tool). Angrepene rammet minst 72 organisasjoner, deriblant våpenleverandører, globale konserner, FN og Den internasjonale olympiske komité (IOC). Valget av angrepsmål (blant annet antidopingbyrået WADA) og timingen (i tiden rundt Beijing-OL i 2008) er blant mange momenter som peker i retning av Kina.

2011: Duqu:
Stuxnets «fetter», med svært mange konstruksjonsmessige likheter trosa ulikt formål. Har hovedfokus på informasjonsinnhenting og har hittil ikke gjentatt Stuxnets herjinger i industrielle Scada-systemer. Ekspertene strides om Duqu er en etterfølger eller en forløper til Stuxnet. Mer sikkert er det at ormen antas å stamme fra samme skapere som Stuxnet.

Figur 4 Faksimile fra TU.no med eksempler fra cyberkrigshistorie

Tabell 2 Eksempler på historiske nasjonale og internasjonale uønskede hendelser knyttet til svikt ved driftskontrollsystemer.

Virus/trojansk hest (Stuxnet) 	Stuxnet (2010) er en dataorm som hadde som hovedmål å sabotere anrikningssentrifuger for uran i et kjernekraftverk i Iran. Det ble spesielt skrevet for å angripe DKS ved anlegget. Stuxnet har evne til å omprogrammere programmerbare logiske styringer (PLS) og skjule endringene. Stuxnet var trolig utviklet av USA/Israel og inkluderte flere såkalte "zero-day" sårbarheter i Windows for å spre seg og/eller infisere DKS programvaren [5, 6]. I følge Nasjonal sikkerhetsmyndighet (NSM) var dette første gang en så trojanere som var spesiallaget for å ta kontroll over prosess- og kontrollsystemene.
Utro tjener/misfornøyd ansatt Maroochy Shire Council	En klassisk hendelse fra Maroochy Shire i Australia fra år 2000. En tidligere innleid IT konsulent som hadde installert DKS som styrte 300 pumpestasjoner for avløp via radiokommunikasjon. Konsulenten fikk ikke jobb i vannverket og hevnet seg ved å manipulere pumpestasjoner og ventiler/-luker slik at en million liter ubehandlet avløpsvann rant ut i nærliggende vassdrag. [5].
Uvedkommende får tilgang til drifts-kontrollsystem til VA-verk via internett 	Publikasjon på internett i november 2011 av skjermdump av brukergrensesnitt fra driftskontroll-systemet til vann og avløpsverket i South Houston Nevada. Uvedkommende skal således ha vært i stand til å endre på driftsparametre ved vannverket. Passord for server tilgjengelig via internett ettersom default passord var benyttet ("100"). http://pastebin.com/Wx90LLum
Skallsikring av anlegg **Kunne stoppet vanntilførselen med mobilen** ** Knusende, hemmelig rapport avslører store svakheter ** Latterlig lett passord beskyttet vann- og avløpssystemet 	Intern revisjon fra kommunen avdekket sårbarheter knyttet til adkomstsikring av vannbehandlingsanlegget ved Oset. Fra media ble det kjent at default passord fra fabrikk var blitt brukt på Bluetooth-enheter. Rapporten medførte økt fokus på informasjonssikkerhet ved VA-verket. Sikkerheten ved anlegget var heldigvis adskillig bedre enn oppslaget i media skulle tyde på. http://www.vg.no/nyheter/utenriks/terrorisme/artikkel.php?artid=10098352

Hendelsene i Maroochy Shire og South Houston viser at dersom passord og brukernavn er tilgjengelig og uvedkommende får tilgang til dem, er det lite som beskytter et drifts-kontrollsystem som er tilgjengelig via internett.

For å illustrere at også store VA-verk kan være sårbare, nevner vi et eksempel fra USA hvor et større VA-verk i California i 2011 ønsket å teste IT-sikkerheten på eget datanettverk. VA-verket leide inn en kjent hacker til å prøve å bryte seg inn. I løpet av en dag hadde hackeren klart å få tilgang til styringen av doseringspumpene for kjemikalier ved vannbehandlingsanlegget. Det svake punktet var at ansatte hadde logget seg på VA-verkets nettverk hjemmefra med private PC'er. Testen viste at den innleide hackeren kunne, dersom han ville, ha gjort drikkevannet til flere millioner mennesker udrikkelig [7].

2.5 Sikkerhetsloven og forskrift om skjermingsverdige objekter innen VA og konsekvenser for driftskontrollsystemer

Forebyggende sikkerhetsarbeid mot trusler som følge av spionasje, sabotasje og terror-handlinger er regulert i Sikkerhetsloven[8]. Det pågår (2013) et arbeid med å peke ut skjermingsverdige objekter etter sikkerhetsloven og objektsikkerhetsforskriften. Innen vann og avløp er det særlig vannforsyning som er relevant for den nye forskriften og det er følgelig særlig her det kan være aktuelt å identifisere skjermingsverdige objekter.

I følge § 17 i sikkerhetsloven skal "*utvelgelse av skjermingsverdig objekt skje på grunnlag av en skadevurdering, der man tar særlig hensyn til objektets betydning for sikkerhetspolitisk krisehåndtering og forsvar av riket, betydning for kritiske funksjoner for det sivile samfunn, symbolverdi og mulighet for å utgjøre en fare for miljøet eller befolkningens liv og helse*".

Hvilke konsekvenser det eventuelt vil få for VA-verket å ha skjermingsverdige objekter er foreløpig uklart. Siden formålet med loven og forskriften er å sikre seg mot sabotasje og terror, vil tiltakene kunne være fysiske, elektroniske og administrative. Dersom noen av anleggene blir kategorisert som skjermingsverdig objekt, vil dette også kunne få direkte konsekvenser for IKT. Det er nærliggende å tro at driftskontrollsystem som utgjør et kritisk styringssystem for VA også vil være en del av det skjermingsverdige objektet. § 3-3 i forskriften sier følgende: "*Dersom tilknytning til internett utgjør en sårbarhet for sikkerheten til et skjermingsverdig objekt, kan Nasjonal sikkerhetsmyndighet (NSM) i samråd med virksomheten og vedkommende departement bestemme at objekteier skal være tilknyttet et sentralt system for varsling av koordinerte angrep via internett. NSM kan gi nærmere bestemmelser om hvordan tilknytningen skal settes opp og forvaltes*." Når det gjelder informasjonssikkerhet er kravene i sikkerhetsloven mest fokusert på beskyttelse av *konfidensialitet*. For de skjermingsverdige objektene er kravene tydelig rettet mot det å sikre funksjonalitet. Her er altså *tilgjengelighetsaspektet* mest fremtredende. Ikke desto mindre vil beskyttelse av konfidensialitet knyttet til forhold ved objektene også være en viktig forutsetning for å sikre tilgjengelighet.

Blant norske vannverk og tilhørende myndigheter diskuteres det (2012-2013) om hvilke vannverk (eventuelt VA-verk) i Norge (om noen i det hele tatt), som skal omfattes av den

nye forskriften. Uavhengig om de enkelte vannverk vil være skjermingsverdige sett ut i fra nasjonale kriterier (viktig for Norges sikkerhet), vil det for hvert enkelt vannverk lokalt uansett være enkelte anlegg (inkludert IKT-systemer for styring og overvåkning av driften) som vil være viktigere enn andre. Dette kan for eksempel være vannbehandlings-anlegg, en stor pumpestasjon som forsyner et viktig område, eller et høydebasseng som forsyner et større område og/eller sårbare abonnenter. Hendelser knyttet til disse anleggene kan medføre at lokalsamfunnet mister tillit til at vannverket kan levere godt og sikkert drikkevann. Per februar 2013 er det ikke kommet noen konklusjon på disse diskusjonene.

3 Årsaker til svikt i driftskontrollsystem

Sikkerhetshendelser skyldes at det både finnes sårbarheter som kan utnyttes og at det finnes en angriper som har motivasjon og evne til å gjennomføre et angrep. I Tabell 3 vises et utvalg sårbarheter som DKS og tilhørende nettverk ofte er utsatt for (tabellen er ikke ment å være uttømmende). I mange tilfeller vil man se at det er flere sårbarheter som virker sammen og gir foranledning til en hendelse.

Tabell 3: Sårbarheter i DKS

Sårbarhet	**Beskrivelse**	**Avbøtende tiltak**
Gamle DKS benyttes	Mangelfull oppgraderinger av DKS. Det benyttes systemer som forutsetter gamle versjoner IT-løsninger	• Hvis fornying ikke er mulig, tilstrebes mest mulig separasjon og isolasjon av (del)systemer.
DKS fornyes sakte og det fortas sjelden en komplett fornyelse	DKS brukes for VA systemer med teknisk lang levetid. Komponentene til VA er også bygget/installert på ulike tidspunkt med ulike tekniske løsninger. Dette gjør at DKS kan bestå av flere generasjoner av kontrollutstyr. Når utstyret er installert er det viktig at DKS har høy tilgjengelighet og oppetid. Det finnes derfor i mange organisasjoner en motvilje mot å utføre endringer i eksisterende systemer som tross alt fungerer. Dette fører til at det tar lang tid før nye sikkerhetsfunksjoner/programoppdateringer installeres.	Se over
Mangelfull dokumentasjon av DKS	Ved endringer av systemet oppdateres ikke dokumentasjonen. Dette gjelder både delsystem, komponenter og eventuelle koblinger mot andre IT system, herunder endringer i kommunikasjon. Dette er viktig også når personell slutter for å sikre dokumentasjon av DKS.	• Innfør en kultur for dokumentasjon i organisasjonen – ingen jobb er ferdig før den er dokumentert. • Legg inn rutine for sluttintervju for å kartlegge hvilket utstyr den ansatte har hatt ansvar for, og vurder om tilstrekkelig dokumentasjon finnes for disse.
DKS er fysisk koblet sammen med administrativt nett	Feil på det administrative nettet påvirker DKS. Dette gjelder også andre veien. Mulighet for uvedkommende å aksessere administrativt nett via DKS og mulighet til å aksessere DKS via administrativt nett.	• Skill DKS fra administrativt nett. • Hvis kobling skyldes tjenestebehov, må tilstrekkelige sikkerhetsmekanismer bygges inn (brannmur, tilgangskontroll, overvåking).

Sårbarhet	Beskrivelse	Avbøtende tiltak
DKS er fysisk koblet sammen med internett	Internett-tilgang fra drifts-kontrollsystem er praktisk for operatør for å være på internett når det er liten aktivitet på driftskontrollsenteret, men dette åpner for at det også lastes ned skadelig kode. Muliggjør uønsket adgang til DKS via internett (virus, hacking).	• Skill DKS fra administrativt nett / internett • Hvis tilkobling skyldes tjenestebehov, sørg for tilstrekkelig dybdeforsvar (dvs. flere sikkerhetsbarrierer, se for øvrig over)
Direkte tilkoblings-muligheter og USB-porter til driftskontroll-system.	Løsningen er enkel og nyttig i forbindelse med oppdatering og annen administrasjon, men muliggjør også at infisert minnepinne kan kobles til DKS direkte. Det var ved bruk av infisert minnepinne at Stuxnet spredte seg til de iranske anrikningsanleggene for uran.	• Fjern ikke benyttede porter.
Bærbare eller stasjonære PC'er som kobles opp utenifra i forbind-else med hjemmevakt kan lett bli infisert av skadelig kode dersom infiserte eller ondartede nettsteder be-søkes.	Enkelte typer nettsteder er mer utsatte enn andre, men det finnes også eksempler på uskyldige nettsteder som via banner-reklamer har spredt virus. Dersom hjemmevakts PC også brukes av familiens andre medlemmer i forbin-delse med nettsurfing og andre aktiviteter, er det store muligheter for infisering av PC. En smittet PC kan der-etter smitte DKS fra innsiden når den kobles til nettverket når en kommer tilbake til jobb.	• Egne PC for hjemmevakt uten annen programvare. • Vurdere behovet for fjernkontroll ut i fra en ROS-analyse. • Ulike rettigheter (tillate mindre muligheter for endring for vann enn for avløp, innsyn i forhold til redigering).
Uklare roller og ansvar for IT-sikkerhet i orga-nisasjonen	Pulverisering av ansvar	• Viktig at IT sikkerhet er satt på dagorden i organisasjonen og at ledelsen prioriterer dette. Dette inkluderer implementering av gode rutiner for IT-sikkerhet/sikkerhetspoli cy i organisasjonen som definerer roller og ansvar.
Mangelfull kunnskap om IT-sikkerhet i orga-nisasjonen	Trusselbildet endrer seg fort innen IT-sikkerhet som en følge av rask utvikling. Stort behov for kontinuerlig etterutdanning. For mindre kommuner/VA-verk kan det være en utfordring å skaffe folk med god IT-kompetanse og en er avhengig av leverandører og konsulenter.	• Opplæring og bevisst-hetstiltak.
Ikke gjennomført ROS-analyser av IKT og DKS innen VA	Egne ROS- analyser av IT sikkerhet og DKS gjennomføres i svært liten grad. Dette har det vært lite fokus på både fra tilsynsmyndighet og blant VA-verkene selv.	• Gjennomfør jevnlige ROS-analyser av både DKS og IKT-systemer.

Sårbarhet	Beskrivelse	Avbøtende tiltak
Dårlige rutiner for å dra lærdom av uhell og nestenulykker knyttet til DKS og IT-sikkerhet	Det er mye lærdom å dra nytte av ved å analysere tidligere IT-relaterte hendelser og nær-svikt.	• Dette inkluderer logging av påloggingsforsøk fra eksterne etc. Viktig med systemer for å registre og følge opp slike hendelser. • Etablere system for registrering av uønskede hendelser knyttet til IKT og DKS.
Lett tilgjengelige vegskap/uteskap som muliggjør tilkobling til nett	Geografisk spredning av VA infrastruktur åpner opp for tilkobling lokalt til utestasjoner (vegskap/uteskap, pumpestasjoner, eller høydebasseng).	• Bedre fysisk sikring av vegskap/uteskap. • Sonedeling av nett.

Tabell 4 gir noen eksempler på kilder til sikkerhetshendelser man kan oppleve i DKS. De fleste av disse kan karakteriseres som sikkerhetsangrep, men i tillegg har vi tatt med ubevisste feil utført av ansatte.

Tabell 4: Kilder til sikkerhetshendelser i DKS

Hendelseskilde	Beskrivelse	Mottiltak
Egne ansatte som gjør ubevisste feil	Ubeviste feil er årsak til mange hendelser.	• Viktig med opplæring og logging.
Egne ansatte som gjør bevisste feil	Egne ansatte kan foreta brudd på sikkerhetsinstruksen av forskjellige årsaker, enten bekvemmelighetshensyn (korrekt prosedyre er for tidkrevende, kjedelig), og/eller fordi ansatte ikke er bevisste på viktigheten av sikkerhetsarbeidet.	• Holdningsskapende arbeid • Viktig med logging for å kunne spore endringene som er utført.
Egne ansatte som utfører bevisste illojale handlinger	Utro tjener	• Viktig med logging for å kunne spore endringene som er utført.
Tidligere ansatte som utfører fiendtlige handlinger	Tidligere ansatte kan fortsatt ha tilgang, og i alle fall kjennskap, til sårbare punkter i IT-systemene og DKS.	• Fjern alle tilgangsrettigheter ved opphør av ansettelsesforhold. • Kontinuerlig vurdering av kjente svakheter i systemet og ytterligere tiltak dersom det er grunn til å tro at svakheter kan utnyttes av tidligere ansatte.
Terrorisme/vandalisme med "politiske" motiv	Eksterne som enten får tilgang til systemene selv (fysisk tilgang eller via hacking) eller tvinger ansatte til å utføre vha. utpressing.	• Tekniske sikkerhetstiltak (brannmur, dybdeforsvar) • Segmentering av tilgangsrettigheter (need-to-know)
Uvilkårlige IT-angrep på DKS	Ikke-målrettede angrep fra virus, f.eks. bivirkninger av Stuxnet.	• Dybdeforsvar • Tekniske mottiltak (antivirus)

3.1 Tilfeldige og utilsiktede feil

For utestasjonene er PLS-feil, lynnedslag, strømsvikt, batterifeil og kommunikasjonsfeil eksempler på tilfeldige og utilsiktede feil. For datasenteret er brann, diskcrash, strøm-brudd, feil med systemet eller backup-systemer typiske tilfeldige og utilsiktede feil. Spesielt kan avhengigheten av nøkkelpersonell og mulig mangel på kompetanse være en sårbarhet.

3.1.1 Teknisk svikt.

Ulike tekniske svikt kan forekomme for alle tilhørende system. Dette inkluderer også svikt i nødvendig kommunikasjon, strømstans og servere.

3.1.2 Naturgitt skade.

Hendelser som skyldes naturlige forhold som vær og vind. Blir ikke spesielt fokusert i denne veilederen.

3.1.3 Menneskelige feil.

Praktisk sikkerhetsarbeid styres i de fleste tilfeller ut fra en tilnærming som bygger på en erkjennelse av at sikkerhet skapes i et samspill mellom menneskelige, teknologiske og organisatoriske faktorer, oftest omtalt som MTO.

Det mest effektive er ikke alene å benytte teknologiske sikkerhetsbarrierer (som virus-kontroll og redundant kommunikasjon), men også basere seg på organisatoriske forhold (etablere prosedyrer, sjekklister, kvalitetssikringsrutiner, godkjenningsordninger, arbeids-kontroll) og forståelse av de mulighetene som ligger i menneskelige faktorer (kompetanse, holdninger og praksis, gi råd til kolleger). IT- sikkerhet knyttet til DKS vil sette særlige krav til forståelse av alarmgrenser og tolkninger av disse. Kompetanse og opplæring er i så måte viktig. For bemannede driftskontrollsystemer har det vært tilfeller der det om sommeren har vært vanskelig å bemanne opp med egne folk og en har da leid inn konsu-lenter som ikke har god erfaring hverken fra IT eller VA. Ved eventuelle hendelser/alarmer som oppstår hvor det må kunne foretas vurderinger av situasjonen og om hvilke tiltak som bør iverksettes, er det derimot viktig med en driftsoperatør som kjenner systemet og hvordan det virker og hva dette vil kunne medføre av bortfall av VA-tjenester.

Menneskelig handling er en direkte årsak eller utløsende faktor til at uønskede hendelser/ulykker oppstår ved at forhold oversees, glemmes eller misforstås, eller ved at operasjoner utføres feilaktig eller i strid med vedtatte prosedyrer eller regelverk. En hendelse trenger ikke være mindre alvorlig selv om årsaken til hendelsen er en ubevisst handling. Generelt kan en skille mellom fire hovedtyper av menneskelig svikt:

- **Feilvurderinger**, forårsaket av manglende kunnskap eller feiltolkninger
- **Feilhandlinger**/operatørfeil
  - Slurv, uoppmerksomhet, forglemmelser
  - Kompetansesvikt - manglende opplæring

- **Utelatelser** – regelbrudd
  - Bevisst
  - Ubevisst

- **Koordineringsfeil**
  - Misforståelser
  - Feilleveranser
  - Manglende kommunikasjon

En vanlig årsak til driftsforstyrrelser av DKS skyldes ubevisste handlinger. Dette kan for eksempel være operatørslurv eller at det gjøres forandringer i systemoppsettet uten at man skjønner konsekvensene av handlingene.

Bevisste (ikke-ondsinnede) handlinger kan ofte medføre store konsekvenser for driften. En god generell sikkerhet i driften av datasystemene slik som beskrevet i denne veiledningen, vil utgjøre en sikkerhetsbarriere også overfor bevisste handlinger.

I enkelte tilfeller kan egne ansatte lures til å slippe uvedkommende inn i DKS elektronisk eller fysisk; dette kan man regne under feilvurderinger, men selve angrepet regnes som bevisst skadeverk (se kapittel 3.2).

3.2 Bevisst skadeverk

Det blir stadig enklere for uvedkommende å tilegne seg kunnskap om DKS. Sårbarheter til standardiserte systemer slik som Microsoft Windows er tilgjengelig via internett. I tillegg finnes det også egne hacker-verktøy/software som kan lastes ned fra internett gratis. Slike gratis programmer er brukervennlige i den forstand at også noviser innen hacking forholdsvis raskt vil kunne bruke verktøyene til å komme inn i VA-verkenes driftskontrollsystem dersom det ligger til rette for det via internett, radio, telefon eller trådløst nett. Slike lett tilgjengelige og brukervennlige hackerverktøy gjør at personer som ønsker å få tilgang til DKS får en kort læretid i forhold til hva situasjonen var før i tiden.

Under bevisst skadeverk regner vi også utro tjenere og sabotasje av forskjellig slag. Dersom det er en på innsiden av egen organisasjon eller en systemleverandør ("insider") som forårsaker handlingen vil de ha svært god kjennskap til kritiske systemer og sårbarhetene i disse. Insidere kan også være egne ansatte som blir manipulert eller truet av eksterne til å gjennomføre bestemte handlinger. De eksterne vil da i praksis være på innsiden av de fleste sikringstiltakene.

Mulige tiltak mht. utro tjenere i egne rekker er å begrense antall brukere som trenger rettigheter for å logge seg på kritiske systemer, gjennomføre sikkerhetssjekk ved ansettelse, påloggingsrutiner med rettighetsbegrensing. Tiltak for å redusere konsekvensene vil også være effektivt, slik som å begrense brukers muligheter til å gjøre feil i systemet ved at ulike brukere har ulike rettigheter.

3.2.1 Generelle angrep

Bruk av hyllevare i DKS, kobling mot Internett og kobling mot bærbare systemer gjør at systemer kan bli utsatt for de generelle IKT-truslene. Eksempler på situasjoner er:

- angrep direkte fra Internett.
- infeksjon på grunn av ansattes surfing på Internett med utstyr som har kritiske funksjoner (f. eks. PC for driftskontrollsystemet som også brukes til å surfe på internett).
- infeksjon fra bærbar enhet som kobles til DKS, utestasjoner og andre installasjoner.

3.2.2 Målrettede angrep

Målrettede angrep kan spenne fra innbrudd/hærverk på utstyr til angrep utenfra via Internett. Noen angrep vil antagelig kreve stor kjennskap til både driftskontrollsystemet og til VA-systemene i seg selv, og vil kun være aktuelle for dedikerte angripere. Det er også mulig å tenke seg angrep på IKT som en del av et større angrep som også inkluderer fysiske angrep. Sannsynligheten for de mest dedikerte angrepene er antagelig liten, men de kan ha store konsekvenser og muligheten bør derfor vurderes. Angripere kan være eksterne eller interne. Eksempler på relevante målrettede angrep:

- Angrep på utestasjoner der angriper er fysisk til stede.
- Angrep på andre deler av VA-systemene fra en utestasjon eller annen del der angriper er fysisk tilstede.
- Angrep på utestasjoner via driftskontrollsystemet, gjerne i kombinasjon med DoS-angrep[4] mot datasenteret slik at det er mindre risiko for å bli oppdaget.
- Angrep mot DKS.
- Angrep mot vannbehandlingsanlegg/avløpsrenseanlegg.
- Angrep for å innhente informasjon som kan brukes for fysiske angrep.
- Angrep mot kommunikasjon/samband.

Særlig viktige aspekter:

- Svakheter ved hjemmevaktordning og oppkobling for fjernkontroll.
- Muligheter for tilgang til systemene for eksterne (leverandører av utstyr) og hvilke sikkerhetskrav som stilles i slike situasjoner.

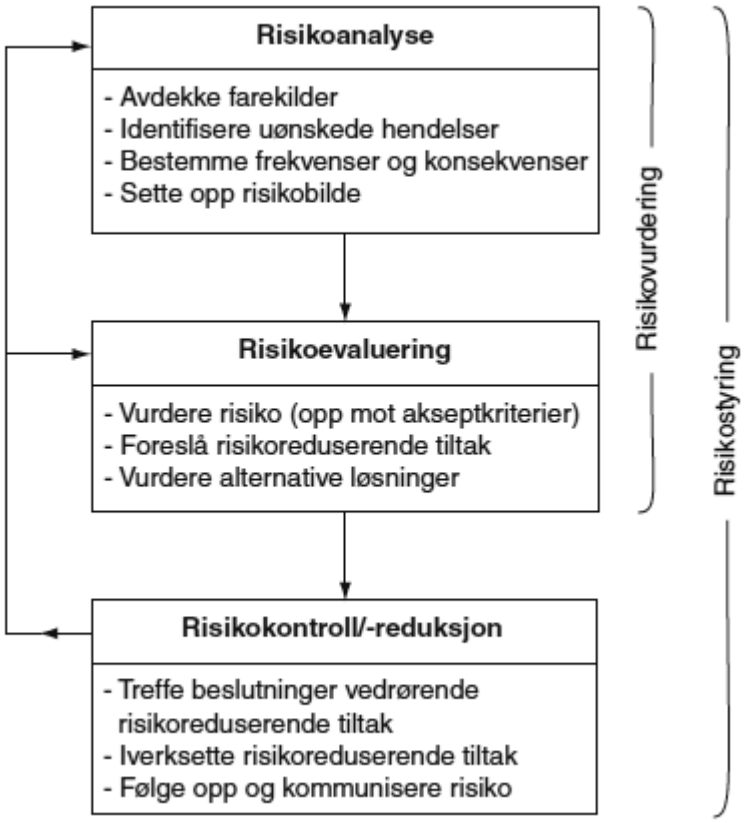
Stuxnet og Duqu er eksempler på virus som er spesialtilpasset spesielle driftskontroll-systemer (Siemens). Det er blant annet ferske eksempler på hacking av VA-verk via driftskontrollsystemet i USA (se kapittel 2.4).

[4] Denial of Service (DoS) (norsk: tjenestenekt-angrep), dvs. hindre normal tjeneste på for eksempel en webserver ved å bombardere den med nettverkstrafikk

4 Helhetlig beredskapskonsept for organisasjonen

For å skape et godt og velfungerende arbeid for sikkerhet i DKS trengs det en god sikkerhetskultur i VA-verket, dvs. en velfungerende håndtering av risiko (risikoanalyse, risikovurdering og risikostyring – se Figur 5) og et systematisk informasjonssikkerhetsarbeid i organisasjonen.

Det er viktig at en basert på lokale ROS-analyser i hvert VA-verk identifiserer de mest kritiske komponenter av VA-systemet (Figur 1) hvor det er særlig viktig at DKS virker. Risikoreduserende tiltak må tilpasses hvert enkelt objekt og hendelse. Kravene til sikkerhet vil variere fra VA-verk til VA-verk og fra komponent til komponent avhengig av lokale forhold og de konsekvenser eventuelt bortfall vil kunne ha. Mattilsynets veileder "Sikkerhet og beredskap i vannforsyningen - veiledning" kan brukes for å etablere et helhetlig sikkerhetskonsept i VA-verket.



Figur 5: Risikostyring som illustrert av Rausand og Utne [9](gjengitt med tillatelse)

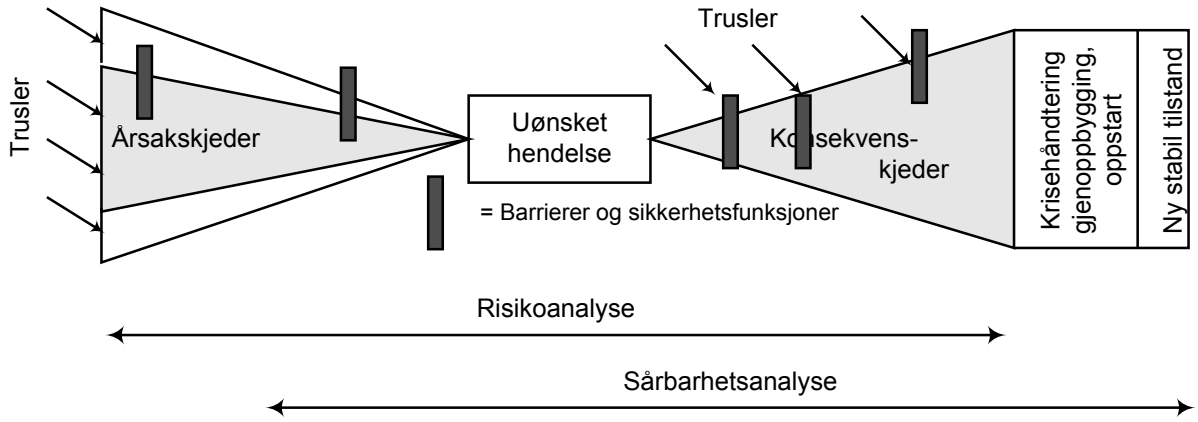
4.1 Risiko og sårbarhetsanalyse

I en risiko og sårbarhetsanalyse er det sentrale temaet å finne ut av hvor lett det er å «slå ut» eller å skade et system. En ROS-analyse av driftskontrollsystem innen VA har som formål å undersøke hvor robust systemet er i forhold til hendelser og trusler slik som virus, strømsvikt og sabotasje. En ROS-analyse kan også omfatte konsekvensene av en systemsvikt.

En ROS-analyse prøver i hovedsak å gi svar på følgende spørsmål:

- Hva kan gå galt knyttet til driftskontrollsystem i VA?
- Hvilke barrierer/tiltak kan redusere sannsynligheten for at noe går galt?
- Hvilke barrierer/tiltak kan redusere konsekvensene hvis noe går galt?

Innholdet i en risiko- og sårbarhetsanalyse er forsøkt illustrert i
Figur 6. Man har ulike trusler som kan forårsake en uønsket hendelse. En slik uønsket hendelse kan igjen ha uønskede konsekvenser. Ulike former for barrierer og sikkerhetsfunksjoner kan anvendes for å redusere sannsynligheten for at truslene forårsaker uønskede hendelser eller for å redusere konsekvensene av slike hendelser. Følgelig kan sikkerhetsbarrierene enten redusere sannsynligheten (S) for den uønskede hendelsen (venstre siden av figuren) og/eller konsekvensene (K) av hendelsen (høyre siden av figuren).



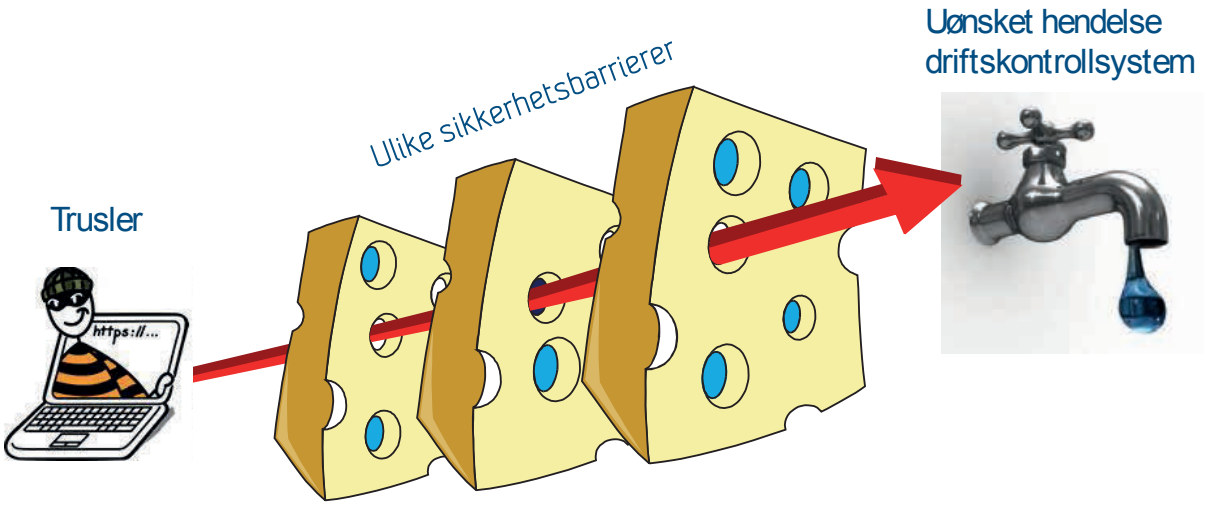
Figur 6: Illustrasjon av en risiko- og sårbarhetsanalyse med trusler (farer), uønskede hendelser, årsaks- og konsekvenskjeder, barrierer og sikkerhetsfunksjoner [9, 10]

Eksempler på tiltak som kan iverksettes for å redusere sannsynligheten for - og konsekvensen av - uønskede hendelser kan være:

- Implementere **fysiske tiltak/planer** (f.eks. etablere skallsikring av anlegg)
- Etablere **driftsrutiner** (f.eks. etablere rutiner for periodisk skifte av personlig passord)
- Fastsettelse av målepunkter/styringspunkter og oppfølging av disse (f.eks logging av avbruddsdata for kommunikasjon for å fange opp trender)

- **Kursing/trening**. Dekker tiltak både i forkant av hendelser for å unngå at hendelsene oppstår og trening i forbindelse med beredskapsøvelser.

For å illustrere at flere sikkerhetsbarrierer må svikte samtidig for at en uønsket hendelse skal opptre, brukes ofte "sveitserostmodellen"
Figur 7), hvor hver enkelt av sikkerhetsbarrierene kan ha svakheter/"hull". Eksempler på sikkerhetsbarrierer er mekanismer som hindrer at en hacker klarer å koble seg på driftskontrollsystemet og modifisere styringen av VA-infrastrukturen på en slik måte at det oppstår uønskede hendelser (pumper stenges av, øke doseringer i prosessanlegg, åpner luker). Disse barrierene kan være materielle/fysiske, menneskelige og organisatoriske. Ulykker skjer når alle hullene i de ulike sikkerhetsbarriererene (osteskiver) ligger på rekke.



Figur 7 "Sveitserost modell" som illustrasjon på flere sikkerhetsbarrierer for driftskontrollsystem

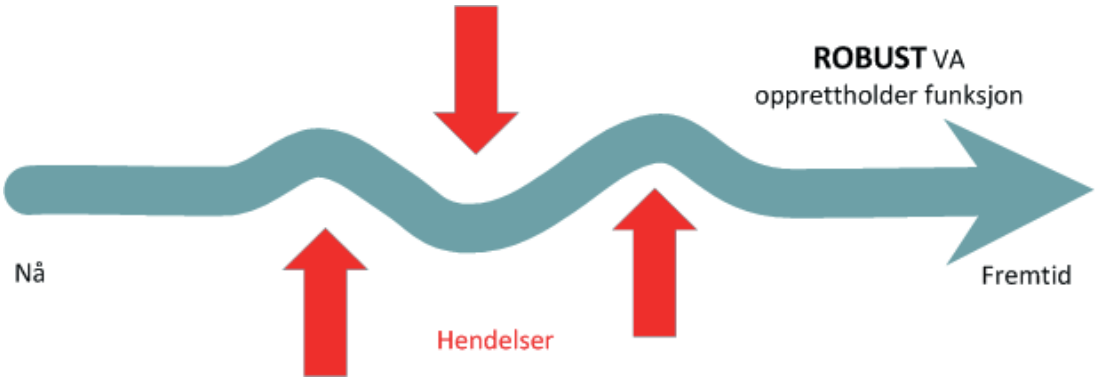
4.2 Mål om robuste VA-systemer

Et hovedmål for vann og avløpssystemene er at de skal være robuste. Dette gjelder også for driftskontrollsystemene knyttet til VA. Et robust VA-system kjennetegnes ved å kunne opprettholde sin funksjon (det å levere godt og nok drikkevann/transportere avløpsvann sikkert bort uten miljømessige konsekvenser) selv om systemet utsettes for ulike typer eksterne og interne trusler/farer. Dette er illustrert i
Figur 8 hvor et VA-system utsettes for ulike typer hendelser/farer, men en klarer likevel å opprettholde funksjonen til VA-systemet som er å levere godt og sikkert drikkevann og transportere og rense avløpsvann.

Typiske kjennetegn ved et robust vann og avløpssystem er følgelig:

- Driftskontrollsystemene er utformet slik at det er vanskelig å få satt de ute av funksjon. Dette gjelder både overfor eksterne (hacking, virus) og interne svakheter som VA-verket selv styrer med.

- Ved bortfall av driftskontrollsystemet skal en fortsatt kunne levere tilfredsstillende VA-tjenester. Konsekvensene av bortfall av driftskontrollsystemet skal altså være så små som mulig. Hva hender dersom driftskontrollsystemet ikke lenger virker? Vil VA-verket fortsatt kunne levere VA-tjenester tilfredsstillende?



Figur 8: Illustrasjon av et robust vann- og avløpssystem som opprettholder sin funksjon selv om det utsettes for farer/trusler.

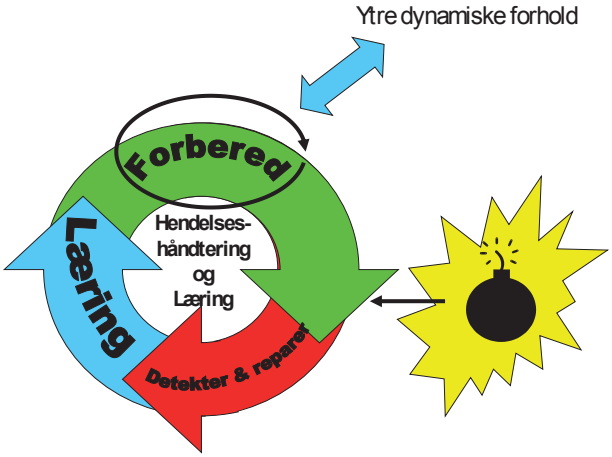
I tillegg til disse kjennetegnene for et robust VA-system og tilhørende driftskontrollsystem, er det også viktig at driftskontrollsystemet raskt kommer opp og går igjen etter en eventuell svikt. Innen pålitelighetsfagfeltet er dette knyttet opp til fagområdet "resiliense" som er knyttet opp mot hvor raskt systemet klarer å bli re-etablert i etterkant av en svikt.

Det må være et mål at driftskontrollsystemene skal bli sikrere og mer robuste slik at de klarer å motstå de fleste hendelser og dersom ulykken likevel skulle oppstå, skal det gå raskt å få systemet opp å gå igjen.

4.3 Hendelseshåndtering

For å kunne tilby robuste driftskontrollsystemer, er det viktig at VA-verket etablerer en strukturert rutine for håndtering av informasjonssikkerhetshendelser når de inntreffer. Gode rutiner kan redusere sannsynligheten for hendelser, men de kan aldri elimineres helt.

Figur 9 illustrerer en tilnærming med 3 faser (basert på [11]); beskrevet i detalj i underkapitlene.



Figur 9: Håndtering av informasjonssikkerhetshendelser

4.3.1 Forberedelsesfasen

Det er viktig at VA-verket har etablert planverk, rutiner og prosedyrer for hvordan den skal reagere på informasjonssikkerhetshendelser. Forberedelsesfasen er en kontinuerlig forbedringsprosess, hvor man innarbeider ny kunnskap fra forskning, sikkerhetsaktører og andre deler av bransjen. I denne fasen vil det også være interaksjon med sikkerhets-arbeidet som drives av andre deler av IT-driftsorganisasjonen ("Ytre dynamiske forhold" i figur 9).

Det er viktig at planverket omfatter både tekniske og ikke-tekniske aspekter [12]. Eksempler på slike aspekter kan være definisjoner på hva som anses som hendelser, klassifisering og prioritering av hendelser og rapporteringsprosedyrer. Det er viktig at prosedyrer for rapportering klart identifiserer hvem som skal varsles, og hvordan dette skal gjøres når en hendelse inntreffer. Videre må det identifiseres hvem som har ansvaret for rapportering i etterkant. Det er viktig at det etableres et eget system for slik rapportering.

For å sikre erfaringsutveksling med andre deler av bransjen bør det etableres formelle[5] møteplasser og rutiner for rapportering av faktiske hendelser. Slike møteplasser og nett-verk kan spille en avgjørende rolle i identifiseringen av eventuelle koordinerte angrep mot bransjen som helhet.

4.3.2 Deteksjons- og reparasjonsfasen

Deteksjon av hendelser kan gjøres både av automatiserte systemer (antivirus eller inntrengningsdeteksjonssystemer) og av ansatte som observerer unormal aktivitet. Personell med ansvar for hendelseshåndtering må gis tilstrekkelig myndighet og ressurser for å løse oppgavene på en effektiv måte. [12]

[5] Selv om møteplassen er formell, viser erfaringer at det ofte er en fordel med en uformell tone i slike sammenhenger.

Det kan være aktuelt å koble DKS fra andre nettverk når en hendelse oppdages, både i tilfeller hvor angrepet kommer utenfra og i tilfeller hvor man ønsker å hindre angrepet fra å spre seg til andre systemer. Etter at en hendelse er isolert og håndtert, er det viktig å gjenopprette normal drift så snart som mulig. Tilkobling til andre nett må vurderes spesielt etter en hendelse og bør kun gjøres når dette er vurdert til å være forsvarlig.

4.3.3 Læringsfasen

Alle hendelser som inntreffer må betraktes som en anledning til å lære, slik at samme hendelse ikke skal kunne skje igjen på samme måte. Gjennomgang og læring må prioriteres av ledelsen, slik at det settes av tid og ressurser til læringsprosessen. Det er også viktig å spre informasjon til andre aktører i bransjen, slik at de i størst mulig grad kan slippe å lære av egne feil.

Erfaringene man trekker ut av læringsfasen mates inn i neste iterasjon av forberedelses-fasen, og kan påvirke rutiner, planverk og/eller tekniske sikkerhetstiltak.

5 Tiltak for å redusere sårbarheten

Tiltakene gjelder både for ledelse og for mer teknisk personale. Tiltakene gjelder både med hensyn til å redusere sannsynligheten til sviktene, men også konsekvensene av hendelsene.

5.1 Retningslinjer for informasjonssikkerhet knyttet til DKS

5.1.1 Virksomheten og DKS henger sammen

Virksomheten må ha generelle retningslinjer for informasjonssikkerhet og i tillegg spesifikke retningslinjer for sikkerhet for DKS som henger uløselig sammen med de generelle retningslinjene.

5.1.2 Organisatorisk IT-sikkerhet

Hva trenger en organisasjon som et VA-verk for å respondere sikkert på utfordringer knyttet til IT sikkerhet? Basert på en modifisering av en generell modell for organisatorisk sikkerhet [13] har vi tilpasset denne til også å gjelde IT-sikkerhet. Et VA-verk som organisasjon må, dersom det skal operere sikkert over tid, utvikle fem ulike sett av organisatoriske egenskaper (se Figur 10):

- Organisasjonen må være **pålitelig**. Det vil si at virksomheten er godt planlagt og styrt, med gode rutiner og tydelige ansvars- og myndighetsforhold fra øverst til nederst i organisasjonen. IT-sikkerhet er altså forankret hos den øverste ledelsen i VA-verket og ledelsen har klart å formidle dette nedover i organisasjonen. Medarbeiderne har IT-kompetanse nok til å håndtere arbeidsoppgavene og kompetansen utvikles etter behov, gjennom opplæring og trening. VA-verk som er pålitelige kjennetegnes av at det normalt gjøres få feil.

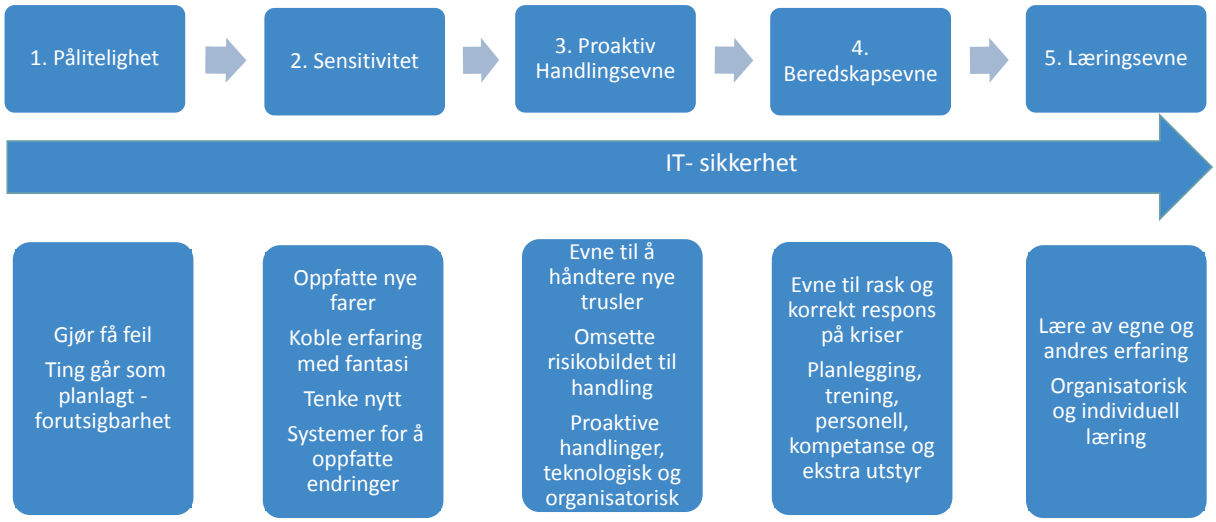
- Organisasjonen må være **sensitiv**. Det vil si at en har prosedyrer, rutiner, praksis og kultur som gjør at en oppdager og forstår mulige faresignaler innenfor eller utenfor virksomheten, også når dette forutsetter at en kombinerer informasjon på nye og ikke-planlagte måter. Nye trusler knyttet til IT sikkerhet fanges opp både eksternt og internt i organisasjonen. Trender i data, slik som økning i antall ikke-autoriserte påloggingsforsøk til DKS, må registreres slik at en tidlig kan fange opp at noe er under utvikling/nye farer.

- Organisasjonen må utvikle **proaktiv handlingsdyktighet**. Det vil si at en har kompetanse, rutiner og reaksjonsevne, slik at tilløp stoppes før de utvikles til mer omfattende og alvorlige hendelser. I mange situasjoner innebærer det at organisasjonen må ha evne til improvisasjon, fordi det kan oppstå situasjoner som en ikke har forestilt seg eller har forberedt seg på. Med proaktiv handlingsdyktighet inkluderes planlegging, iverksetting av forebyggende tiltak og nødvendig organisering for å kunne håndtere ekstraordinære situasjoner.

- Organisasjonen må ha **reaktiv handlingsdyktighet/beredskapsevne**. Det vil si at en må være i stand til å håndtere hendelser og ulykker som uansett måtte

inntreffe, slik som tekniske sammenbrudd, brann, eller terrorhandlinger. Dette inkluderer også evne til å gjenopprette funksjonene slik at DKS rask kommer opp og går igjen etter en hendelse.

- Organisasjonen må ha **evne til læring**. Det vil si at en må være i stand til å registrere og analysere ulykker og hendelser og bruke dette som grunnlag for både formell og uformell erfaringsoverføring og læring. Det er også viktig å trekke lærdom ut av det som går som det skal. Videre er det viktig at erfaringer fra beredskapsøvelser systematiseres og at ny kunnskap og erfaringer implementeres inn i DKS.



Figur 10: Modell for organisatorisk IT-sikkerhet (inspirert av [10])

Et sentralt poeng her er at de ulike kapabilitetene/evnene forutsetter ulike organisatoriske egenskaper, fordi det ikke er noen nødvendig sammenheng mellom disse. En veldrevet byråkratisk organisasjon kan operere pålitelig og «uten feil», men være dårlig rustet til å oppdage tilløp som ikke er definert inn som noens bestemte ansvarsområde, eller som fordrer at en kombinerer informasjon fra ulike kilder på måter som det ikke finnes prosedyrer eller rutiner for. En tilsynelatende robust organisasjon kan også vise seg å være ute av stand til å håndtere uventede hendelser dersom disse forutsetter evne til improvisasjon.

5.1.3 Basis for sikkerhetspolitikken

Virksomhetens generelle sikkerhetspolitikk skal være basert på god praksis for informasjonssikkerhet [14] og tilhørende krav for styringssystem for informasjonssikkerhet [15].

5.1.4 Grunnleggende premiss for DKS sikkerhetspolitikk

Det grunnleggende premisset for den DKS-spesifikke sikkerhetspolitikken skal være at tiltak fremstår for de ansatte som en logisk utvidelse av den generelle sikkerhetspolitikken.

5.1.5 Fysisk beskyttelse
Den DKS-spesifikke sikkerhetspolitikken skal også omfatte fysisk beskyttelse av DKS og tilhørende nettverk.

5.1.6 Ansvar
Sikkerhetsansvar, oppgaver og myndighet for DKS-miljøet skal forkynnes og konkretiseres for administratorer og brukere av DKS.

5.1.7 DKS integrert i risikohåndtering
DKS-miljøet omfattes som en integrert del av risikohåndteringsprosessen på høyeste nivå i virksomheten.

5.2 Sikkerhetsbevissthet

5.2.1 Bevissthetsprogram
Virksomheten skal ha et kontinuerlig sikkerhetsbevissthetsprogram for sine ansatte.

5.3 Revisjon

5.3.1 Årlig revisjon
DKS og tilhørende nettverk skal være gjenstand for revisjon minst en gang i året. Revisjonen bør inneholde en systemteknisk verifikasjon på at sikkerhetsmekanismene faktisk er implementert og fungerer etter hensikten.

5.3.2 Ekstern revisjon
I tillegg til interne revisjoner bør det også periodisk utføres systemtekniske revisjoner av en uavhengig tredjepart.

5.4 Anskaffelsespolitikk for driftskontrollsystemer og –tjenester

Det er lettest å sørge for at systemer har tilstrekkelige sikkerhetsmekanismer når de anskaffes; det er vesentlig vanskeligere (noen ganger umulig) og dyrere å ettermontere sikkerhetsmekanismer på eksisterende utstyr.

5.4.1 Opprettholdelse av drift
Ved inngåelse av kontrakt med leverandører av (store) DKS bør det vurderes om det skal være en klausul vedrørende reservedeler og støtte for å sikre leveranse og kvalitet på drikkevann:

- Leverandøren må lagerføre et tilstrekkelig antall reservedeler for et nærmere avtalt antall år.
- Leverandøren må garantere at den kan tilby bistand for å finne løsninger i forbindelse med katastrofer.
- Hvis DKS og/eller tilhørende nettverk går tapt, vil leverandøren uavhengig av årsak tilby prioritert bistand til erstatning av DKS og/eller nettverk.
- Leverandøren skal verifisere oppdateringer fra tredjeparter som tilbyr vesentlige systemkomponenter (f.eks. Microsoft Windows operativsystemer) innen et rimelig tidsrom og skal gjøre slike oppdateringer tilgjengelige på en tiltrodd og pålitelig måte.

Dersom leverandør ikke kan garantere lagerhold av reservedeler og at VA-verket vurderer at tilgjengelige reservedeler er kritisk for å kunne opprettholde sikkert drift, må VA-verket vurdere om det selv skal stå for slik lagerføring. Se for øvrig også avsnitt 5.5.29.

5.4.2 Minimumskrav

Før anskaffelse skal virksomheten spesifisere informasjonssikkerhetskrav som DKS, nettverk og programvare er forventet å oppfylle. Se også kap. 12 i «God praksis for informasjonssikkerhet» [14]. Den virksomhetsspesifikke risikoanalysen som skal utføres i forkant av anskaffelsen vil også avdekke konkrete krav til integritet og konfidensialitet i disse systemene.

Ved anskaffelse av DKS er det viktig å definere krav til systemet på forhånd med hensyn til sikkerhet. Hovedspørsmålet som må besvares er:

- *Hvor viktig er DKS for VA-verket?*
- *Hvilke krav til "oppetid" skal det stilles til anlegget?*
- *Hvor mange dager eventuelt timer kan anlegget være ute av drift før konsekvensene for forbrukerne og miljøet blir uakseptable.*

Dette vil være avhengig av de lokale forholdene ved hvert enkelt VA-verk. Dersom et VA-verk har store rentvannsbasseng som kan levere drikkevann i flere døgn, er bortfall av DKS mindre kritisk enn dersom en har bare har rentvannsbasseng som tilsvarer noen timers vannforbruk. I det siste tilfellet vil det følgelig være viktigere at DKS raskt re-etableres ved utfall.

Det må også settes mål og krav til valg av kvalitet på kommunikasjonstjenester (grad av redundans, tilknytningspunkt på nettet, kommunikasjonstype etc.). Noen telekommunikasjonsleverandører leier nett fra andre leverandører. VA-verkets behov til kommunikasjonsløsning og grad av redundans må komme klart frem i avtaler med leverandører av telekommunikasjonstjenester. Dette gjøres ved å utarbeide bindende avtaler som beskriver kvalitet på tjenestene (Service Level Agreement). Kommunikasjon i forhold til

integritetsbeskyttelse og konfidensiell overføring av data (kryptering) er også viktig. Ulike kommunikasjonsløsninger har ulike IT-sikkerhetsutfordringer.

Foruten tekniske krav til DKS og kommunikasjon er det også viktig med fysisk sikring av bygget hvor utstyret er lokalisert. Dette gjelder forhold som sikring mot brann, varme, avbruddsfri strømforsyning (UPS) og adkomstsikring.

5.4.3 Drift & vedlikehold fra tredjepart

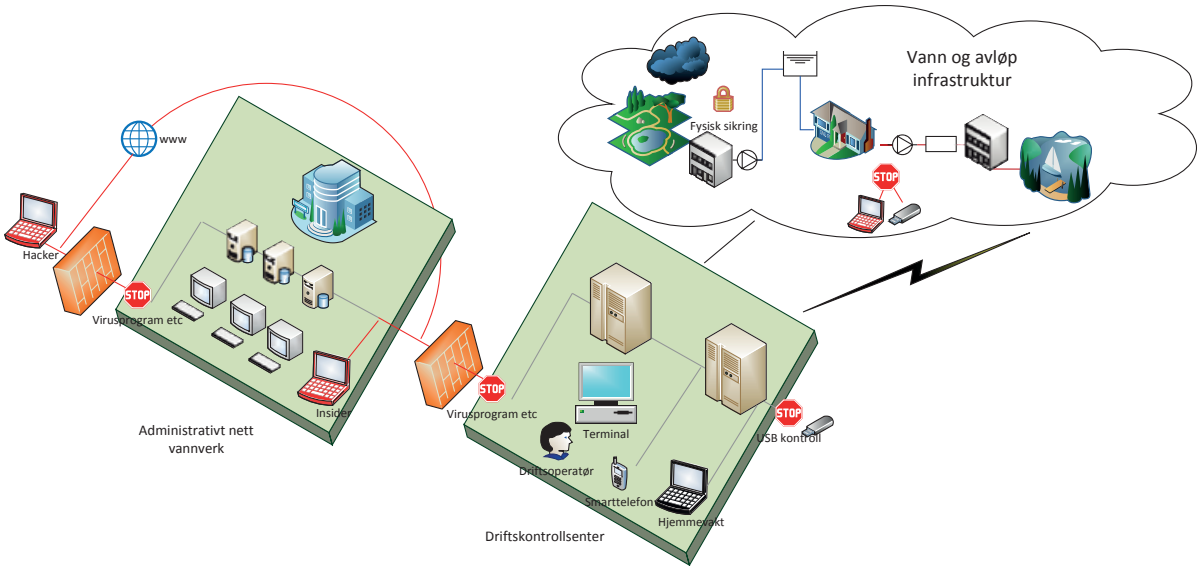
Drift & vedlikeholdskontrakter med tredjeparter skal ha en sikkerhetsklausul som minst omfatter:

- Drift- og vedlikeholdspersonell skal etterleve virksomhetens gjeldende sikkerhetspolitikk for DKS og nettverk.
- Klarering og tilgangsavtaler for driftspersonell.
- Garantier for forsvarlig behandling av virksomhetens sensitive/graderte informasjon.
- Overvåking/oppfølging av arbeid som skal utføres av tredjeparter på vegne av virksomheten.

Ved behov for oppgraderinger av DKS må det kartlegges om dette kan gjøres lokalt eller om systemleverandør krever mulighet for fjernoppkobling. Det er ofte vanlig at leverandør av driftskontrollsystem får tilgang å utføre endringer på systemene via Internett fra egen bedrift. En slik tilgang bør bare tillates dersom det foretas en grundig sikkerhetsgjennomgang av teknisk løsning og personellet som skal utføre arbeidet. Dersom det gis mulighet for ekstern tilgang fra leverandør, bør denne kunne åpnes og lukkes ved behov, f.eks. ved å gi tilgang fra et gitt tidspunkt i et bestemt antall timer.

5.5 Tekniske sikringstiltak

I følgende underkapitler beskrives kortfattet en del anbefalte tekniske sikringstiltak. Mange av tiltakene er illustrert i Figur 11. Ytterligere tiltak for sikring av nettverk er spesifisert i NSMs veiledning i nettverkssikkerhet [12].



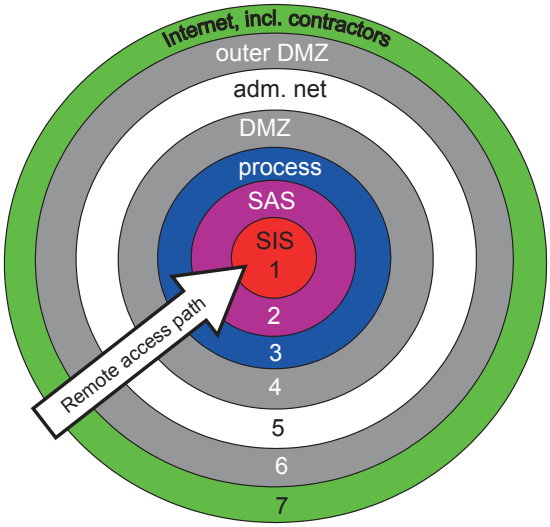
Figur 11 Illustrasjon sikring av DKS (Fritt etter Melissa Hegge, www.tu.no (2012))

5.5.1 Brannmur

DKS må sikres mot andre nett ved hjelp av brannmur. DKS kan også med fordel segmenteres internt ved bruk av brannmurer.

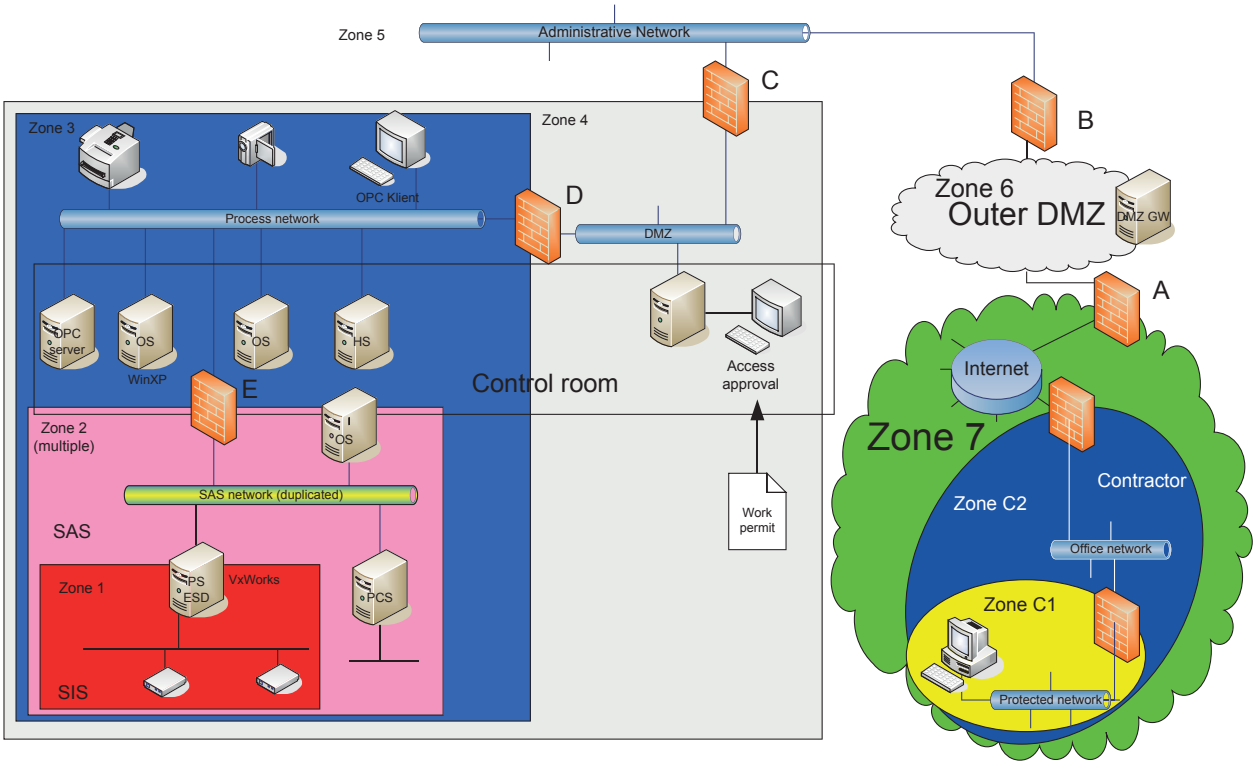
5.5.2 Dybdeforsvar

DKS-miljøet skal organiseres etter prinsippet om dybdeforsvar (*defense in depth*). Dette kan konseptualiseres som en løk [16], der det er sikringstiltak for hvert lag av løken (se Figur 12). På samme måte som løken har flere lag skal sikkerheten av DKS bestå av flere sikkerhetsbarrierer som beskytter systemene på flere nivåer. For eksempel vil en sonedeling av datanettverket medføre at skadelig kildekode (virus) bare slår ut deler av nettet og en har mulighet til å isolere denne delen.



Figur 12: Eksempel på dybdeforsvar – løkmodell [16]

Et eksempel fra et prosesskontrollmiljø[11] er vist i Figur 13. I dette eksempelet opererer vi med flere såkalte demilitariserte soner (DMZ) – dette er nettverkssegmenter mellom to brannmurer som i utgangspunktet ikke skal ha ordinært datautstyr, og følgelig heller ikke ordinær trafikk.



Figur 13: Eksempel på DKS-nettverk med dybdeforsvar (hentet fra SeSa prosjektet i SINTEF, "The SeSa Method for Assessing Secure Remote Access to Safety Instrumented Systems")[16].

Dybdeforsvar medfører at det er flere lag av sikkerhet, og at de mest kritiske komponentene (dvs. de instrumenterte sikkerhetssystemene i eksempelet i Figur 13) ikke kan aksesseres uten å forsere multiple sikkerhetsmekanismer.

I tillegg til soner i dybden, bør man også vurdere å segmentere deler av nettverket på tvers, slik at deler av systemet som ikke har behov for å kommunisere sammen, heller ikke kan nås direkte fra hverandre.

5.5.3 Separat DKS og kontornettverk

DKS-miljøet er sikret og holdt separat fra kontormiljøet. Dette er også illustrert i Figur 13, der kontormiljøet er i sone 5. Som illustrert i Figur 13 bør man, mellom administrativt nettverk og DKS, i tillegg til brannmur, også ha en DMZ. All kommunikasjon mellom administrativt nett og DKS bør følgelig gå via tjenester i DMZ; dette omfatter også fjernaksess-løsninger som beskrevet i avsnitt 5.5.9.

5.5.4 Reell mulighet til å koble DKS fra kontornettverket

Når DKS og kontormiljø er skikkelig separert, vil det, i tilfelle trafikkoverbelastning eller eksternt angrep, være mulig å koble DKS fullstendig fra andre nettverk [11].

5.5.5 Sikre forbindelser til DKS-nettverk

Fjern alle DKS-forbindelser som ikke er essensielle. Alle data-porter som det ikke er bruk for bør fjernes. Basert på ROS-analyser av det enkelte VA-anlegg, kan kryptering av kommunikasjon vurderes.

5.5.6 Revisjon av forbindelser

Med utgangspunkt i den gjeldende sikkerhetspolitikk, gjennomføres grundig og kontinuerlig kontroll med alle gjenværende forbindelser og informasjon som passerer gjennom dem.

5.5.7 Internett

For mange kommunale VA-verk forvaltes internett ofte administrativt sentralt i kommunen. Dette inkluderer systemer for logging av data, valg av tekniske løsninger, og brannmurer. I slike tilfeller er det viktig at VA-verkets IT-personell arbeider tett med de sentrale IT- medarbeiderne i kommunen for å sikre gode løsninger som også tar hensyn til VA-verkets og driftskontrollsystemenes behov. Det er for kommunen mer kritisk om kritiske driftskontrollsystemer faller ut, enn at de ansatte sentralt i kommunen ikke får tilgang til internett og administrative servere for lagring av dokumenter.

DKS bør ikke kobles direkte til internett eller andre åpne nettverk. Funn fra en svensk spørreundersøkelse [4] viste at DKS til bruk innen vannforsyning i stor utstrekning var fysisk knyttet til administrative IT-nett i VA-verket. Det var også vanlig å være tilknyttet IT-systemet til leverandøren av driftskontrollsystemet. Undersøkelsen slo også fast at tilgang til Internett direkte fra driftskontrollsystemet var vanlig.

Hvis det er behov for å overføre rapporteringsdata til eksterne leverandører, bør det vurderes å gjøre dette via enveisforbindelser som ikke kan utnyttes av eksterne angripere [12, 17]. Dersom man ikke bruker enveisforbindelser bør man:

- Konfigurere ekstern overføring slik at forbindelsen initieres fra DKS til ekstern leverandør.
- Konfigurere brannmur/DMZ slik at initiering motsatt vei blokkeres.
- Overføringen bør sikres med kryptering.

Tiltaket for VA-verket vil være å vurdere om nettverket for driftskontroll kan separeres fra administrative systemer. Direkte tilgang til internett fra driftskontrollsystemet er også en sårbarhet som bør fjernes dersom det eksisterer i dag.

5.5.8 Overføring via åpne nett

Dersom DKS skal bruke internett eller andre åpne nettverk for overføring av informasjon, bør slike beslutninger tas basert på separat risikoanalyse med hensyn på effekten av tjenestenektangrep (*Denial of Service*) og tap/bortfall av den åpne nettinfrastrukturen.

Grunnregel: ikke overføring av informasjon i åpne nett uten bruk av krypterte forbindelser

Også private kabelforbindelser som fysisk går gjennom områder som virksomheten ikke har direkte kontroll over må betraktes som åpne i denne forbindelse og følgelig kun benyttes til kryptert kommunikasjon.

5.5.9 Fjernaksess fra åpne nett

Dersom DKS skal kunne fjernaksesseres fra internett eller andre åpne nettverk, bør en slik beslutning være basert på en separat risikoanalyse som konkluderer med at dette er forsvarlig.

Dersom det tillates fjernaksess fra åpne nett kreves det at:

- Kun autorisert utstyr underlagt konfigurasjonskontroll tillates tilkoblet fjernaksess.
- Det skal gjøres tilleggsautentisering vha. en tofaktor autentiseringsmekanisme (f.eks. brukernavn/passord og kodegenerator som illustrert i Figur 14).

Figur 14: Eksempel på kodegeneratorenhet[6] brukt i tofaktor autentisertingssystem.

- Den eksterne forbindelsen skal krypteres slik at hverken passord eller andre data sendes i klartekst.
- Det skal foretas gjensidig autentisering av klient og tjener, f.eks. ved hjelp av digitale sertifikater på tjeneren (evt. også på klient).
- Det skal være en egen DMZ sone i brannmur tilegnet fjernaksess.
- Det skal defineres et maksimum antall uriktige påloggingsforsøk (typisk: 3), før fjerntilgang låses for et nærmere bestemt tidsrom (typisk: 30 minutter) for et

[6] http://www.flickr.com/photos/dailylifeofmojo/3499428617/

bestemt brukernavn. Ved ytterligere feil økes sperretiden proporsjonalt. Ved sperring av bruker skal det gis alarm til IT-personell.

- Det skal etableres logging av påloggingsforsøk, med minimum registering av IP-adresser og tidspunkt.

- Dersom et stort antall påloggingsforsøk med ulike brukernavn registreres fra samme IP-adresse, skal det genereres alarm til IT-personell.
- Tilgangslogger skal analyseres jevnlig.

- Det må sikres at IT-ansatte har tilstrekkelig opplæring til å analysere serverdata og loggfiler.

Mer utfyllende krav kunne vært definert, men dette vil inngå i et inntrengnings-deteksjonssystem ("intrusion detection system" - IDS) som er spesialprogramvare/system som følger med trafikken på nettverket og logger unormale hendelser.

5.5.10 Trådløse nett

DKS bør ikke ha trådløse aksesspunkter (Wi-Fi) med mindre det er utført en separat risikoanalyse (med bistand) av sikkerhetseksperter som konkluderer at risikoen er akseptabel.

5.5.11 Modem

Modem eller andre eksterne aksesspunkter skal overvåkes kontinuerlig, og utstyres med en pålitelig og sterk autentiseringsmekanisme. Autorisasjoner for fjernaksess bør gjennomgås jevnlig (f.eks. årlig) for å se om det fortsatt eksisterer et behov. Behov skal dokumenteres før ekstern tilgang innvilges. Det skal benyttes tilbakeringing og kun autoriserte nummer skal ligge i listen.

5.5.12 Sikkerhetskomponenter

Sikkerhetstiltak og innstillinger til nettverkskomponenter som tilbyr sikkerhetsmekanismer (brannmur, ruter, VPN) skal gjennomgås og verifiseres regelmessig (årlig).

5.5.13 Sikre DKS og nettverkskomponenter

DKS skal være "herdet" ved installering slik at kun de maskinvare/programvare-komponenter som brukes er tilgjengelige og DKS sikkerhetsmekanismer som tilbys fra leverandør skal utnyttes til det fulle.

5.5.14 Dokumentasjon av konfigurasjon

Konfigurasjonsprosessen til DKS og tilhørende nettverk skal være dokumentert. Virksomheten bør derfor til enhver tid ha oppdatert dokumentasjon av driftskontroll-systemet, samt en oversikt over alle sikkerhetstiltak som er implementert. Dette bør inkludere en oppdatert skjematisk fremstilling av driftskontrollsystemets logiske og fysiske

nettverk som viser alle eventuelle tilgangspunkt mellom driftskontrollsystemet og andre nettverk. En oversiktlig skjematisk fremstilling vil kunne være til stor hjelp for virksomhetene for å ha oversikten over eget system, og til hjelp under situasjoner med feilrettingssituasjoner i DKS.

5.5.15 Konfigurasjonskontroll

Endringer i konfigurasjon for DKS skal være en kontrollert prosess. Konfigurasjonskontroll er kontroll av den funksjonelle og fysiske sammensetningen av maskin- og programvare i DKS og har som mål å unngå at endringer i godkjent konfigurasjon medfører redusert sikkerhet. Konfigurasjonskontroll i et sikkerhetsaspekt skal registrere og analysere endringer i maskinvare, programvare, nettverksarkitektur og brukere.

5.5.16 Antivirus

I den grad det er mulig, skal DKS beskyttes av oppdatert antivirus-programvare. I tillegg bør all kommunikasjon mellom DKS og andre nettverk skannes for virus og andre former for skadevare (engelsk: *malware*).

5.5.17 Oppdatering

Det skal formuleres en rutine for oppdatering og "lapping" (engelsk: *patching*[7]) av DKS og tilhørende nettverkskomponenter, som er i henhold til en akseptabel risiko i forhold til angrep fra inntrengere, virus og andre former for skadevare.

5.5.18 Sikker beskyttelse av DKS-miljøet

Bare autorisert personell skal ha fysisk og elektronisk tilgang til DKS og tilhørende nettverk.

Utestasjonene innen VA er spredt over et stort geografisk område. Dette vanskeliggjør fysisk sikring av alle utestasjoner. For større utestasjoner slik som pumpestasjoner, høydebasseng og prosessanlegg er det som regel gode systemer for adkomstsikring som sensorer i dørlås, bevegelsesdetektor, alarm, autentisering med bluetooth-nøkkel eller mobiltelefon og kameraovervåkning.

For de mindre utestasjonene som også er tilknyttet DKS kan ofte adkomstsikringen være enklere. Dette gjelder særlig målepunkter i kummer hvor PLS kan være lokalisert i egne vegskap/uteskap som åpnes med en enkel nøkkel. Dersom en ikke har tilstrekkelig sonedeling av nettet, vil uvedkommende kunne koble seg direkte til PLS og videre til VA-verkets interne nett og driftskontrollsystemet. Et mulig tiltak for å sikre enkle vegskap/uteskap kan være å etablere alarmsignal på om skapdør er åpen. Sonedeling av nett slik at for eksempel et skadelig virus ikke kan spre seg til hele nettet, er et annet nyttig tiltak for å redusere konsekvensene. En sonedeling vil også kunne begrense skaden som kan utføres av en inntrenger som får fysisk tilgang til en enkelt utestasjon, som nevnt i avsnitt 5.5.1.

[7] Patching (norsk : lapping): brukerrettet og ekstraordinær «lapping» av ferdig programvare typisk for å fikse en feil.

5.5.19 Autorisert utstyr

Bare forhåndsautorisert utstyr får tilkobles DKS-nettverket. Utstyr som benyttes i driftskontrollsystemet tillates ikke brukt i andre nettverk eller løsninger utenom drifts-kontrollsystemet. Virksomheten skal ha en effektiv kontrollordning for sikker avhendig av utstyr som har blitt benyttet i driftskontrollsystemet. Sikker avhending innebærer at virksomheten må kontrollere at all informasjon om driftskontrollsystemet og annen sensitiv informasjon er betryggende slettet før utstyret avhendes.

Porter som ikke er i bruk på switcher og annet nettverksutstyr må deaktiveres. Tilkoblet utstyr bør utstyres med kommunikasjonsalarm som varsler dersom det kobles fra, slik at man kan få generert alarm dersom noen forsøker å koble fra autorisert utstyr og koble til uautorisert utstyr.

Det skal ikke være tillatt å bruke personlig eid utstyr i driftskontrollsystemet (BYOD- bring your own device). Personlig utstyr er sjelden omfattet av virksomhetenes sikkerhets- og kontrollregime og kan derfor være mer mottakelig for ondsinnet programvare.

5.5.20 Utstyr fra tredjeparter

Utstyr fra tredjeparter (bærbare datamaskiner, nettbrett, o.l.) bør som hovedregel ikke tilkobles DKS-nettverk eller andre nettverk i virksomheten. Hvis det gjøres unntak fra denne regelen, bør utstyret/programvaren i hvert enkelt tilfelle gjennomsøkes med oppdatert antivirusprogramvare før tilkobling. Tilkobling kan for eksempel kun skje under oppsyn av en ansatt i virksomheten, som følgelig blir ansvarlig.

5.5.21 Passordpolitikk for DKS

Alle standard brukernavn/passord satt av leverandøren skal umiddelbart endres til verdier valgt av virksomheten ved installasjon av programvare/systemer.

Forslag til enkle passordrutiner:

- Passord skal ikke deles med andre.
- Passord skal ikke skrives ned, unntak kan være nedskrevne passord som oppbevares i en safe med begrenset tilgang eller passord som lagres kryptert i egne passord-applikasjoner.
- Passord skal skiftes minst hver tredje måned.
- Passord skal ha en lengde og kompleksitet som gjør dem vanskelige å gjette
  - Passord skal være minst 8 tegn
  - Passord skal ikke bestå helt eller delvis av ord som kan finnes i en ordliste
  - Passord bør bestå av store og små bokstaver, tall og spesialtegn

Når ansatte slutter i bedriften må brukernavn sperres og passord slettes slik at ikke informasjonen kan brukes til pålogging av systemene.

Passord til sentrale systemfunksjoner:

- Skal være komplekse (se eksempler gitt ovenfor)
- Skal bare gis til ansatte med tjenstlig behov
- Skal endres jevnlig (minst hver tredje måned)

I tillegg til krav til passord må det selvfølgelig være egne brukernavn for hver enkelt bruker.

5.5.22 Personlige passord og kontroll med brukertilgang

I så kritiske systemer som driftskontrollsystem må virksomheten ha kontroll med hvem som har tilgang, hvilke funksjoner de har lov til å utføre og når de har vært pålogget. Særlig viktig er det at virksomheten har rutiner for å slette tilgangen for personer som slutter eller ikke lenger skal arbeide med driftskontrollsystemet. Tilgangsrettigheter bør gjennomgås årlig for å sikre at alle tilgangsrettigheter er korrekte og på riktig nivå. Det er viktig at man ved undersøkelser etter uønskede hendelser kan gå tilbake i loggene og se hvem som var pålogget da hendelsen oppstod.

Det skal alltid brukes personlige brukernavn og passord med tilhørende rettigheter for tilgang til systemet. For å gjøre bruken av passord lettere for brukeren, kan VA-verket benytte moderne forvaltningssystemer for passordbruk inkludert "single-sign-on" hvor de ansatte kan forholde seg til alle jobbsystemene med kun ett passord.

5.5.23 Forretningskontinuitet for DKS og nettverkskomponenter

Styringssystemet for opprettholdelse av aktivitet for DKS og nettverkskomponenter skal være konstruert i henhold til kapittel 14 av god praksis for informasjonssikkerhet [14]. Et viktig aspekt ved dette systemet er at virksomheten har en godt vedlikeholdt kriseplan for alle kritiske komponenter i DKS-miljøet og at denne planen er gjenstand for jevnlige øvelser.

5.5.24 Sikkerhetskopiering

Kritiske data i DKS og nettverkskomponenter skal sikkerhetskopieres jevnlig. Dette kan løses ved å foreta daglig inkrementell sikkerhetskopiering (for utstyr som støtter dette), samt ukentlig komplett sikkerhetskopiering av alle data. Valg av tidsintervall vil følge av en ROS-analyse og de konsekvenser som kan oppstå.

Det anbefales at alle servere konfigureres med speiling av harddisker (f.eks. RAID 1[8]), slik at fysisk skade på en enkelt harddisk ikke medfører tap av data.

[8] Raid 1: speiling av disker slik at det som skjer på den ene disken skjer også med den andre. På denne måten sikrer en at dersom den ene harddisken skulle ryke, er den andre 100% oppdatert og arbeidet kan fortsette uten opphold. Virker bare mot mekaniske feil i diskene, og sikrer rask oppe-tid.

5.5.25 Lagring av sikkerhetskopi

Sikkerhetskopier av DKS-informasjon skal lagres sikkert på en annen fysisk plassering enn DKS. Ved for eksempel brann i bygningen hvor DKS er lokalisert, er det viktig at sikkerhetskopier ikke er lagret i samme bygning.

5.5.26 Verifisering av sikkerhetskopier

Det skal inngå, som en del av kvalitetsarbeidet, å verifisere at sikkerhetskopier kan brukes i en gjenopprettingsoperasjon. Det er ikke nok å ta en sikkerhetskopi av databasen for siden å håpe at sikkerhetskopien virker når en trenger den. En sikkerhetskopi som ikke er forsøkt gjenopprettet må betraktes som en ikke-eksisterende sikkerhetskopi.

5.5.27 Administrasjon av lagringsmedia i DKS-miljøet

Lagringsmedier brukt i DKS-miljøet må administreres effektivt på en kontrollert måte gjennom hele livsløpet, også i forbindelse med avhending/destruering. Ulike metoder for sletting/destruksjon av lagringsmedia er aktuelle.

5.5.28 Krav til strømforsyning til driftskontrollanlegg

Alle kritiske funksjoner må være knyttet til avbruddsfri strømforsyning (UPS). En egen risikovurdering må gjennomføres for å avgjøre om det i tillegg må være nødstrøm tilgjengelig i tilfelle av langvarig strømbrudd. Dersom avbruddsfri strømforsyning er kritisk, er det viktig at UPS kan levere strøm inntil nødstrømsanlegg har starter opp. Oppstartstid for et nødstrømsanlegg kan typisk være ½ min og i denne perioden må UPS anlegget levere strøm. At UPS faktisk virker etter intensjonen kan enkelt testes ved å ta strømmen.

5.5.29 Reparasjonsberedskap

For en del av årsakene til svikt vil det være aktuelt med en diskusjon knyttet til hvor lang tid det tar å få reparert/reetablert komponenten (Mean Time To Repair - MTTR). Dette arbeidet vil sees i sammenheng med årsakene til svikt. De typiske mest kritiske komponenter vil bli identifisert med tilhørende estimat over typiske reparasjonstider (kort tid, lang tid).

Avhengighet av enkeltleverandører kan reduseres dersom alle moduler og kommunikasjonsgrensesnitt beskrives i tilstrekkelig detalj til å kunne foreta reparasjoner med generiske komponenter. Dette stiller i så fall store krav til dokumentasjonen.

5.6 Sjekkliste for sikre driftskontrollsystemer innen vann og avløp

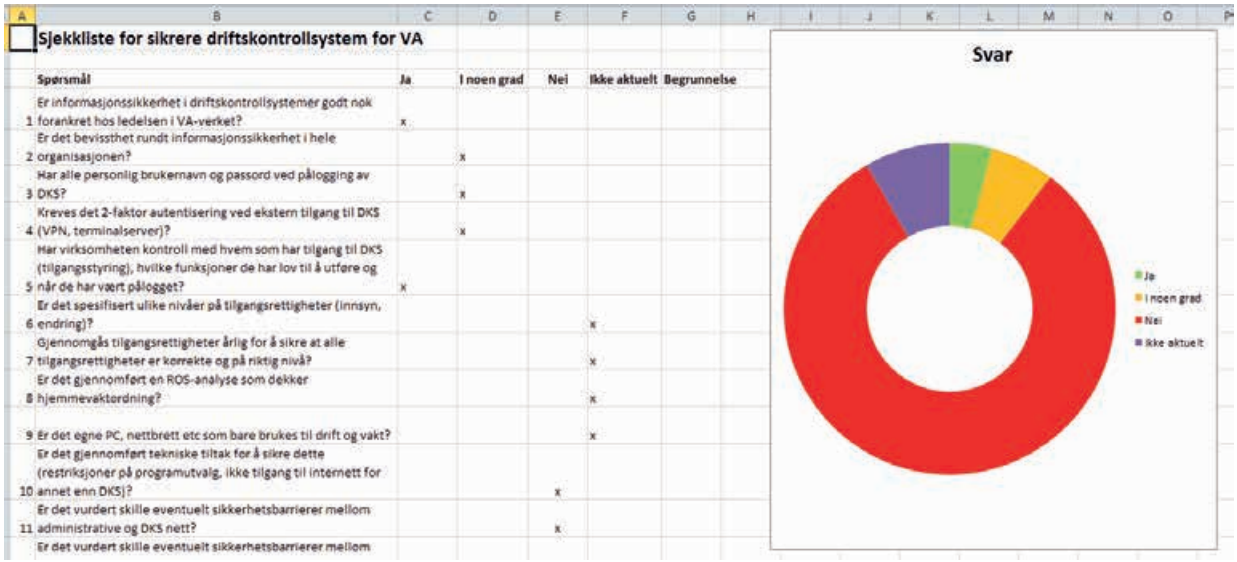
I prosjektet er det utarbeidet en enkel sjekkliste som kan brukes for å sjekke ut sikkerhet knyttet til DKS innen VA. Sjekklisten er også utformet som et enkelt regneark som vist i

Figur 15. Regnearket følger vedlagt den digitale versjonen av rapporten og kan lastes ned fra *www.norskvann.no*.

Svaralternativene til hvert spørsmål er: ***Ja, Nei, vet ikke, ikke aktuelt***.

- Er informasjonssikkerhet i driftskontrollsystemer godt nok forankret hos ledelsen i VA-verket?
- Er det bevissthet rundt informasjonssikkerhet i hele organisasjonen?
- Har alle personlig brukernavn og passord ved pålogging av DKS?
- Er alle standardpassord fjernet?
- Er det krav til tilstrekkelig styrke på passord?
- Er det krav til regelmessig bytte av passord?
- Kreves det 2-faktor autentisering ved ekstern tilgang til DKS (VPN, terminalserver)?
- Har virksomheten kontroll med hvem som har tilgang til DKS (tilgangsstyring), hvilke funksjoner de har lov til å utføre og når de har vært pålogget?
  - Vurdering av de som har intern / ekstern tilgang til systemer. (Vandelsattest / taushetsplikt)
- Er det spesifisert ulike nivåer på tilgangsrettigheter (innsyn, endring)?
- Gjennomgås tilgangsrettigheter årlig for å sikre at alle tilgangsrettigheter er korrekte og på riktig nivå?
- Er det gjennomført en ROS-analyse som dekker hjemmevaktordning?
- Er det egne PC, nettbrett etc. som bare brukes til drift og vakt?
- Er det gjennomført tekniske tiltak for å sikre at dedikert utstyr ikke brukes til andre ting (restriksjoner på programutvalg, ikke tilgang til internett for annet enn DKS)?
- Er det vurdert skille, eventuelt sikkerhetsbarrierer mellom administrative og DKS nett?
- Er det vurdert skille, eventuelt sikkerhetsbarrierer mellom internett og DKS?
- Har VA-verket vurdert kritikaliteten/viktigheten av de ulike utestasjoner/VA-anlegg?
- Er det egne DKS-nett for henholdsvis vann og avløp (sonedeling)?
- Er det foretatt *geografisk* sonedeling av DKS nett?
- Er det mekanismer som begrenser muligheten til å få tilgang til andre deler av DKS fra hvilken som helst utestasjon?
- Finnes det et system for registrering av hendelser og avvik i virksomheten?
- Finnes det et eget system for systematisk registrering av hendelser og avvik (svikt) for DKS?
  - Evt. er det hensiktsmessig å registrere DKS hendelser og avvik i det generelle avvikssystemet
- Finnes det nedskrevne rutiner for håndtering av hendelser og avvik i DKS?
- Er det lett for uvedkommende å få innsyn i opplysninger om geografisk plassering av VA-infrastruktur?
- Har en sikret redundans av kritiske systemer/komponenter (to servere, kommunikasjon, strømforsyning, datarom)?

- Er det noen anlegg som ikke kan driftes i manuell modus når man mister kontakt med utestasjonene (vannbehandlingsanlegg)?
- Finnes det avtaler for informasjonssikkerhet mot eksterne driftsleverandører?
- Finnes det systemer for inntrengningsdeteksjon (IDS)?
- Finnes det rutiner/mekanismer for viruskontroll mot DKS?
- Finnes det rutiner for oppdatering/patching av systemer i DKS?
- Har VA-verket gjennomført en analyse av DKS koblinger mot andre system (Internett, administrative system etc) som kan utgjøre en fare?
  - Vurdering av sikkerhet i de forskjellige nettverk / radiosamband
- Dekker beredskapsplanen også DKS hendelser?
- Er beredskapsplanen blitt oppdatert siste år?
- Er det tilstrekkelig skallsikring av VA-infrastruktur slik at det ikke er for enkelt å få fysisk adgang til infrastrukturen?
- Står den fysiske sikringen av anleggene i forhold til viktigheten av VA-anleggene?
- Er det gode rutiner for å sikre tilstrekkelig opplæring og videreutdanning av personell i informasjonssikkerhet?
- Gjennomføres det periodiske ROS analyser i VA-verket som i tilstrekkelig grad også fokuserer på informasjonssikkerhet og DKS?
- Har VA-verkets beredskapsøvelse også inkludert IKT/DKS hendelser?
- Har VA-verket beredskap og forberedte tiltak for alternativ drift av VA-systemet ved svikt i hele eller deler av driftskontrollsystemet?
- Har VA-verket tilstrekkelig egen kompetanse innen informasjonssikkerhet og DKS, eller er de helt avhengig av leverandører og konsulenter?
- Har VA-verket en avtale om full backup av konfigurasjon av DKS?
- Har VA-verket tilstrekkelig faglig bestillerkompetanse ved nyanskaffelser av DKS?
- Har man satt krav til oppe-tid for DKS?
- Er alle systemløsningene og beskrivelsene av DKS godt dokumentert?
  - Systemdokumentasjon
  - nettverksdiagram
  - strømforsyningsdiagram
  - datautveksling mot eksterne enheter
    - andre DKS
    - verdier for vedlikeholdssystem (FDV)
    - rapportering,
    - VPN
- Foretas det periodisk oppdatering av system / DKS dokumentasjon?
- Gjennomføres periodiske tester av DKS for å sjekke at anlegget fungerer etter intensjonen? Ref. internkontroll som skal inkludere f.eks måleverdiene som rapporteres er det riktige og algoritmene for styring er korrekt og etter planen.



Sjekkliste for sikrere driftskontrollsystem for VA

	Spørsmål	Ja	I noen grad	Nei	Ikke aktuelt	Begrunnelse
1	Er informasjonssikkerhet i driftskontrollsystemer godt nok forankret hos ledelsen i VA-verket?	x				
2	Er det bevissthet rundt informasjonssikkerhet i hele organisasjonen?		x			
3	Har alle personlig brukernavn og passord ved pålogging av DKS?		x			
4	Kreves det 2-faktor autentisering ved ekstern tilgang til DKS (VPN, terminalserver)?		x			
5	Har virksomheten kontroll med hvem som har tilgang til DKS (tilgangsstyring), hvilke funksjoner de har lov til å utføre og når de har vært pålogget?	x				
6	Er det spesifisert ulike nivåer på tilgangsrettigheter (innsyn, endring)?				x	
7	Gjennomgås tilgangsrettigheter årlig for å sikre at alle tilgangsrettigheter er korrekte og på riktig nivå?				x	
8	Er det gjennomført en ROS-analyse som dekker hjemmevaktordning?				x	
9	Er det egne PC, nettbrett etc som bare brukes til drift og vakt?				x	
10	Er det gjennomført tekniske tiltak for å sikre dette (restriksjoner på programutvalg, ikke tilgang til internett for annet enn DKS)?			x		
11	Er det vurdert skille eventuelt sikkerhetsbarrierer mellom administrative og DKS nett?			x		
	Er det vurdert skille eventuelt sikkerhetsbarrierer mellom					

Figur 15. Enkel sjekkliste utformet som et regneark brukt til å kartlegge sikkerhet i driftskontrollsystem. Figuren fremkommer av svarene. Regnearket kan lasts ned fra www.norskvann.no

6 Referanser

[1] E. Luiijf, "SCADA Security Good Practices for the Drinking Water Sector," TNO TNO-DV 2008 C096, 2008.

[2] I. V. Malvik, A. Rogstad, R. Arnulf, H. Ulsberg, T. Sønsteby, F. Skapalen, R. Steen, B. Høegh, and A. Gjengstø, "Forslag til revidering av regelverket for beredskap i energiforsyningen og forslag til forskrift om forebyggende sikkerhet og beredskap i energiforsyningen (beredskapsforskriften)," Norges vassdrags- og energidirektorat, 2012.

[3] P. Radmand, A. Talevski, S. Petersen, and S. Carlsen, "Taxonomy of Wireless Sensor Network Cyber Security Attacks in the Oil and Gas Industries," in *Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on*, 2010, pp. 949-957.

[4] E. Johansson, "Kartläggning av SCADA-säkerhet inom svensk dricksvattenförsörjning," SvensktVatten rapport C29 120, 2010.

[5] E. Chien. (2011, last accessed October 2012). W32.Stuxnet Dossier. *Security Response Blog*. Available: http://www.symantec.com/connect/blogs/w32stuxnet-dossier

[6] J. Slay and M. Miller, "Lessons Learned from the Maroochy Water Breach," in *Critical Infrastructure Protection*. vol. 253, E. Goetz and S. Shenoi, Eds., ed: Springer Boston, 2007, pp. 73-82.

[7] K. Dilanian, "Virtual war a real threat," Los Angeles Times, March 28, 2011 http://articles.latimes.com/2011/mar/28/nation/la-na-cyber-war-20110328

[8] *Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven),* Forsvarsdepartementet, 1998. Available: http://www.lovdata.no/all/nl-19980320-010.html

[9] M. Rausand and I. B. Utne, *Risikoanalyse. Teori og metoder*. Trondheim: Tapir Akademisk Forlag 2009.

[10] M. Rausand, *Risk Assessment; Theory, Methods, and Applications*: Wiley, 2011.

[11] M. G. Jaatun, E. Albrechtsen, M. B. Line, O. H. Longva, and I. A. Tøndel, "A Framework for Incident Response Management in the Petroleum Industry," *International Journal of Critical Infrastructure Protection,* vol. 2, pp. 26-37, April 2009.

[12] "N-01 Network Security Guidance - Guidance on Network Security to comply with the NSM Information Security directive," NSM, 2012. Available: https://www.nsm.stat.no/Documents/Veiledninger/N-01%20Network%20Security%20Guidance.pdf

[13] P. M. Schiefloe, "En modell for samfunnssikkerhet.," NTNU Samfunnsforskning AS, 2012.

[14] ISO/IEC, "Information technology - Security techniques - Code of practice for information security management " ISO/IEC 27002, 2005.

[15] ISO/IEC, "Information technology - Security techniques - Information security management systems - Requirements," ISO/IEC 27001, 2005.

[16] T. O. Grøtan, M. G. Jaatun, K. Øien, and T. Onshus, "The SeSa Method for Assessing Secure Remote Access to Safety Instrumented Systems," SINTEF A1626, 2007. Available: http://sintef.org/SeSa

[17] M. G. Jaatun, T. O. Grøtan, and M. B. Line, "Secure remote access to autonomous safety systems: A good practice approach," *International Journal of Autonomous and Adaptive Communications Systems,* vol. 2, 2009.

Utgitte Norsk Vann Rapporter

(Tidligere kalt NORVAR-rapporter)

20. Slambehandling og -disponering ved større kloakkrenseanlegg. Sluttrapport
20a. Slambehandling og -disponering ved større kloakkrenseanlegg. Aerob og anaerob behandling
20b. Slambehandling og -disponering ved større kloakkrenseanlegg. Kalking. Kompostering
20c. Slambehandling og -disponering ved større kloakkrenseanlegg. Slamavvanning
20d. Slambehandling og -disponering ved større kloakkrenseanlegg. Termisk behandling av kloakkslam
21. NORVAR's årsberetning 1991
22. EDB i VAR-teknikken. Fase 1 - kravspesifikasjoner m.m. Status-beskrivelse og forslag til videre arbeid *(Utgått)*
23a. Internkontroll for VA-anlegg. Mal for internkontroll-håndbok for VA-anlegg.
23b. Internkontroll for VA-anlegg. Internkontrollhåndbok for avløpsanlegg. Eksempel fra Fredrikstad og omegn avløpsanlegg
23c. Internkontroll for VA-anlegg. Internkontrollhåndbok for vannverk. Eksempel fra Vansjø vannverk
23d. Aktivitetsstyrende håndbok for VA-anlegg. Informasjon, avvik og tiltak, verne- og sikkerhetsarbeid, opplæring
23e. Aktivitetsstyrende håndbok for VA-anlegg. HMS ved vannbehandlingsanlegg
23f. Aktivitetsstyrende håndbok for VA-anlegg. HMS ved avløpsrenseanlegg
23g. Interkontroll for VA-anlegg. Eksempel på driftsinstruks Oltedalen kloakkrenseanlegg
23h. Internkontroll for VA-anlegg. Eksempel på driftsinstruks Smøla vannverk
23i. Internkontroll for VA-anlegg. Internkontroll for VA-transportsystemet. Eksempel fra Nedre Eiker kommune
24. NRV-prosjekt. Korrosjonskontroll ved vannbehandling med mikronisert marmor
25. Mal for prosessoppfølging av anlegg for stabilisering og hygienisering av slam
26. Installering av gassmotor for strømproduksjon ved renseanlegg
27. Mottak og behandling av avvannet råslam ved renseanlegg som hygieniserer og stabiliserer slam i væskeform
28. Slam på grøntarealer. Erfaringer fra et demonstrasjonsprosjekt
29. Regnvannsoverløp
30. Utvikling og uttesting av datasystem for informasjonsflyt i VA-sektoren *(Utgått)*
31. PRO-VA, Brukerklubb for prosess-styresystemer, drift- og fjernkontroll for VA-anlegg. Oversikt pr.1993. Leverandører, produkter, konsulenter *(Utgått)*
32. Bruk av statiske metoder (kjemometri) for å finne sammenhenger i analyseresultater for avløpsvann
33. Evaluering av enkle rensemetoder. Slamavskillere
34. Evaluering av enkle rensemetoder. Siler/finrister
35. Kravspesifikasjon og kontrollprogram for VA-kjemikalier *(Utgått)*
36. Filter som hygienisk barriere
37. EU/EØS, konsekvenser for Norges vannforsyning
38. NORVAR-prosjekter 1992/93 *(Utgått)*
39. Implementering av EDB-basert vedlikeholdssystem. Erfaringer fra referanseprosjekt knyttet til pilot-prosjekt ved Bekkelaget renseanlegg *(Utgått)*
40. Driftsassistanser for avløp. Utredning om rolle og funksjon fremover
41. Metri-tel. Kommunikasjonsmedium for VA-installasjoner. Erfaringer fra prøveprosjekt i Sandefjord kommune *(Utgått)*
42. Industriavløp til kommunalt nett. Evaluering av utførte industrikartleggingsprosjekt.
43. Korrosjonskontroll ved Hamar vannverk
44. Slam på grøntarealer. Erfaringer fra et demonstrasjonsprosjekt. Vekstsesongen 1994
45. Forsøk med forfelling og felling i 2 trinn med polyaluminium-klorid høsten 1993 Kartlegging av slam- slamvannsstrømmer med og uten forfelling 1993-94
46. Renovering av avløpsledninger. Retningslinjer for dokumentasjon og kvalitetskontroll
47. Strategidokument for industrikontroll
48. NORVAR og miljøteknologi. Forprosjekt
49. Grunnundersøkelser for infiltrasjon - små avløpsanlegg. Forundersøkelse, områdebefaring og detaljundersøkelse ved planlegging og separate avløpsanlegg *(Erstattet av 178/10)*
50. Rørinspeksjon i avløpsledninger. Rapporteringshåndbok *(Erstattet av 145/05)*
51. Slambehandling
52. Bruk av slam i jordbruket
53. Bruk av slam på grøntarealer
54. Rørinspeksjon av avløpsledninger. Veileder *(Erstattet av 145/05)*
55. Vannbehandling og innvendig korrosjonskontroll i vannledninger
56. Vannforsyning til næringsmiddelindustrien. Krav til kvalitet. Vannverkenes erstatningsansvar ved svikt i vannleveransen
57. Trykkreduksjon. Håndbok og veileder
58. Karbonatisering på alkaliske filter
59. Veileder ved utarbeidelse av prosessgarantier
60. Avløp fra bilvaskeanlegg til kommunalt renseanlegg
61. Veileder i planlegging av fornyelse av vannledningsnett
62. Veileder i planlegging av spyling og pluggkjøring av vannledningsnett
63. Mal for godkjenning av vannverk
64. Driftserfaringer fra anlegg for stabilisering og hygienisering av slam i Norge
65. Forslag til veileder for fettavskillere til kommunalt avløpsnett
66. EØS-regelverket brukt på anskaffelser i VA-sektoren
67. Filter som hygienisk barriere - fase 3
68. Korrosjonskontroll ved Stange vannverk
69. Evaluering av enkle rensemetoder, fase 2. Siler/finrister
70. Evaluering av enkle rensemetoder, fase 2. Store slamavskillere samt underlag for veileder
71. Evaluering av enkle rensemetoder, fase 3. Veileder for valg av rensemetode ved utslipp til gode sjøresipienter
72. Utviklingstrekk og utfordringer innen VA-teknikken. Sammenstilling av resultatet fra arbeidet i NORVARs gruppe for langtidsplanlegging i VA-sektoren
73. Etablering av NORVARs VA-infotorg. Bruk av internett som kommunikasjonsverktøy *(Utgått)*
74. Informasjon fra NORVARs faggruppe for EDB og IT. Spesialrapport - 5. Utgave Beskrivelse av 34 EDB-programmer/Moduler for bruk i VA-teknikken *(Erstattet av 133/03)*
75. NORVARs faggruppe for EDB og IT. IT-strategi i VA-sektoren. *(Erstattet av 133/03)*
76. Dataflyt-klassifisering av avløpsledninger. *(Erstattet av 150/07)*
77. Alternative områder for bruk av slam utenom jordbruket. Forprosjekt
78. Alternative behandlingsmetoder for fettslam fra fettavskillere
79. Informasjonssystem fordrikkevann, forprosjekt
80. Sjekklister/veiledninger for prosjektering og utførelse av VA-hoved og stikkledninger - sanitærinstallasjoner
81. Veileder. Kontrahering av VA-tekniske prosessanlegg i totalentreprise
82. Veileder for prøvetaking av avløpsvann
83. Rørinspeksjon med videokamera. Veiledning/rapportering *(Erstattet av 145/05)*
84. Forfall og fornyelse av ledningsnett
85. Effektiv partikkelseparasjon innen avløpsteknikken
86. Behandling og disponering av vannverksslam. Forprosjekt
87. Kalsiumkarbonatfiltre for korrosjonskontroll. Utprøving av forskjellige marmormasser
88. Vannglass som korrosjonsinhibitor. Resultater fra pilotforsøk i Orkdal kommune
89. VA-ledningsanlegg etter revidert plan- og bygningslov
90. Actiflo-prosjektet ved Flesland ra
91. Vurdering av slamfabrikk" for Østfold
92. Informasjon om VA-sektoren - forprosjekt
93. Videreutvikling av NORVAR. Resultatet av strategisk prosess 1997/98
94. Nettverksamarbeid mellom NORVAR, driftsassistanser og kommuner
95. Veileder for valg av riktige sensorer og måleutstyr i VA-teknikken *(Erstattet av 192/12)*
96. Rist- og silgods - karakterisering, behandlings- og disponeringsløsninger
97. Slamforbränning (VA-forsk 1999-11). (Samarbeidsprosjekt med VAV)
98. Kvalitetssystemer for VA-ledninger. Mal for prosessen for å komme fram til kvalitetssystem som tilfredsstiller kravene i revidert plan- og bygningslov
99. Veiledning i dokumentasjon av utslipp
100. Kvalitet, service og pris på kommunale vann- og avløpstjenester
101. Status og strategi for VA-opplæringen
102. Oppsummering av resultater og erfaringer fra forsøk og drift av nitrogenfjerning ved norske avløpsrenseanlegg
103. Returstrømmer i renseanlegg. Karakterisering og håndtering
104. Nordisk konferanse om nitrogenfjerning og biologisk fosforfjerning 1999
105. Sjekkliste plan- og byggeprosess for silanlegg
106. Effektiv bruk av driftsinformasjon på renseanlegg/mal for rapportering
107. Utslipp fra mindre avløpsanlegg. Teknisk veiledning. Foreløpig utgave

108. Data for dokumentasjon av VA-sektorens infrastruktur og resultater
109. Resultatindikatorer som styringsverktøy for VA-ledelsen
110. Veileder i konkurranseutsetting. Avtaler for drift og vedlikehold av VA-anlegg
111. Eksempel på driftsinstruks for silanlegg. Cap Clara i Molde kommune
112. Erfaringer med nye renseløsninger for mindre utslipp
113. Nødvendig kompetanse for drift av avløpsrenseanlegg. Læreplan for driftsoperatør avløp
114. Nødvendig kompetanse for drift av vannbehandlingsanlegg. Læreplan for driftsoperatør vann
115. Pumping av avløpsslam. Pumpetyper, erfaringer og tikk
116. Scenarier for VA-sektoren år 2010
117. VA-juss. Etablering og drift av vann- og avløpsverk sett fra juridisk synsvinkel *(Erstattet av 134/03)*
118. Veiledning for kontrahering av rådgivnings- og prosjekteringstjenester innen VAR- teknikk *(Erstattet av 138/04)*
119. Omstruktureringer i VA-sektoren i Norge En kartlegging og sammenstilling
120. Strategi for norske vann- og avløpsverk. Rapport fra strategiprosess 2000/2001
121. Kjøkkenavfallskverner for håndtering av matavfall. Erfaringer og vurderinger
122. Prosessen ved utarbeidelse av miljømål for vannforekomster. Erfaringer og råd fra noen kommuner
123. Utslipp fra mindre avløpsanlegg. Veiledning for utarbeidelse av lokale forskrifter
124. Nødvendig kompetanse for legging av VA-ledninger. Læreplan for ADK 1
125. Mal for forenklet VA-norm
126. Organisering og effektivisering av VA-sektoren. En mulighetsstudie
127. Vassdragsforbund for Mjøsa og tilløpselvene - en samarbeidsmodell
128. Bruk av resultatindikatorer og benchmarking i effektivitetsmåling av kommunale VA-virksomheter. Erfaringer og anbefalinger fra et prøveprosjekt
129. Rørinspeksjon med videokamera. Veiledning/rapportering hovedledninger
130. Gjenanskaffelseskostnadene for norske VA-anlegg
131. Effektivisering av avløpssektoren
132. Forslag til nytt system for prosjektvirksomheten i NORVAR
133. IT-strategi for VA-sektoren. Veiledning
134. VA-JUS. Etablering og drift av vann- og avløpsverk sett fra juridisk synsvinkel *(Oppdateres årlig på www.norskvann.no)*
135. Vannledningsrør i Norge. Historisk utvikling. 26 dimensjonstabeller
136. Hygienisk barrierer og kritiske punkter i vannforsyningen: Hva har gått galt?
137. Veiledning i bygging og drift av drikkevannsbasseng *(erstattet av 181/2011)*
138. Veiledning for kontrahering av rådgivnings- og prosjekteringstjenester innen VAR-teknikk. Revidert utgave
139. Erfaringar med klorering og UV-stråling av drikkevatn
140. NORVARs videre arbeid med slam. Strategisk plan for prosjektvirksomhet, informasjon og kommunikasjon. Forprosjekt
141. Trenger Norge en VA-lov? Drøfting av behovet for en egen sektorlov for vann og avløp
142. NORVARs benchmarkingsprosjekt 2004 Presentasjon av målesystem og resultater for 2003 ed analyse av datamaterialet
143. Kartlegging av mulig helserisiko for abonnenter berørt av trykkløs vannledning ved arbeid på ledningsnettet
144. Veiledning i overvannshåndtering *(Erstattet av 162/08)*
145. Inspeksjonsmanual for avløpssystemer. Del 1 – Ledninger
146. Bærekraftig vedlikehold. Betraktninger av utvalgte problemstillinger knyttet til langsiktig forvaltning av vannledningsnett
147. Optimal desinfeksjonspraksis for drikkevann
148. Veiledning i utarbeidelse av prøvetakingsprogrammer for drikkevann
149. Tilførsel av industrielt avløpsvann til kommunalt nett. Veiledning
150. Dataflyt – Klassifisering av avløpsledninger
151. Veiledning for vedlikeholdssystemer (FDV)
152. Veiledning for anskaffelse av driftskontrollsystemer i VA-sektoren
153. Norm for symboler i driftskontrollsystemer for VA-sektoren
154. Norm for tagkoding i VA-anlegg
155. Norm for merking og FDV-dokumentasjon i VA-sektoren
156. Veiledning for oljeutskilleranlegg
157. Organiske miljøgifter i norsk avløpsslam. Resultater fra undersøkelsen i 2006/07
158. Termoplastrør i Norge – før og nå
159. Håndbok i kildesporing i avløpssystemet
160. Driftserfaringer med membranfiltrering
161. Helsemessig sikkert vannledningsnett
162. Veiledning i klimatilpasset overvannshåndtering
163. Veiledning for innhenting og evaluering av tilbud på analyseoppdrag
164. Veiledning for UV-desinfeksjon av drikkevann
165. Innsamlingsverktøy for vedlikeholdsdata
166. Tiltak for å bedre fosforfjerningen på kjemiske renseanlegg
167. Veiledning for kjøp av VA-kjemikalier
168. Veiledning for dimensjonering av avløpsrenseanlegg
169. Optimal desinfeksjonspraksis fase 2
170. Veileder til god desinfeksjonspraksis
171. Erfaringer med lekkasjekontroll
172. Trykktap i avløpsnett
173. Veiledning for bruk av støpejernsrør
174. Hygienisering av avløpsslam. Langtidslagring og enkel rankekompostering. Resultater fra 3 års valideringstesting
175. Vann og avløp for nye i bransjen – læreplan E-læring og samlinger
176. Statlige gebyrer og avgifter på de kommunale VAR-tjenestene
177. Drikkevannskvalitet og kommende utfordringer – problemoversikt og status
178. Grunnundersøkelser for infiltrasjon – mindre avløpsanlegg
179. Veiledning i utarbeidelse av kommunale gebyrforskrifter for vann og avløp
180. Fjernavlesning av vannmålere
181. Veiledning i bygging og drift av drikkevannsbasseng
182. Prøvetaking av avløpsvann og slam
183. Veiledning om regulering av VA-tjenester til næringsmiddelindustri
184. Tilsyn med utslipp fra avløpsanlegg innen kommunens myndighetsområde
185. Fett i avløpsnett. Kartlegging og tiltaksforslag
186. Veiledning i omorganisering av andelsvannverk til samvirkeforetak
187. Kommunal overtakelse av vannverk organisert som andelslag eller samvirkeforetak
188. Veiledning for drift av koaguleringsanlegg
189. Håndbok for driftsoptimalisering av koaguleringsanlegg
190. Klimatilpasningstiltak innen vann og avløp i kommunale planer
191. Rettigheter til uttak av vann til allmenn vannforsyning
192. Veiledning for valg av riktige sensorer og måleutstyr i VA-teknikken
193. Veiledning i dimensjonering og utforming av VA-transportsystem
194. Energiriktig design og prosjektering av avløpsrenseanlegg
195. Sikkerhet og sårbarhet i driftskontrollsystemer for VA-anlegg

Rapportserie B:

B1: Effektive VA-organisasjoner og tilfredse brukere. Forprosjekt
B2: PressurePuls for deteksjon av lekkasje på vannledninger.
B3: Kvalitetsheving av nye VA-ledningsanlegg. Kartlegging og tiltaksforslag
B4: Vannkvalitet i ledningsnett – Problemoversikt og status. Forprosjekt.
B5: Utslipp fra bilvaskehaller
B6: Kommunikasjonsstrategi for NORVAR og norske vann og avløpsverk
B7: Sandnesmodellen. Eksempel på system for kommunikasjon og virksomhetsstyring
B8: Forprosjekt energinettverk i VA-sektoren
B9: Utvikling av et system for spørreundersøkelser blant VA-kundene
B10: Vannkilden som hygienisk barriere
B11: Økonomiske forhold i interkommunalt VA-samarbeid – praksis og kjøreregler
B12: Drikkevatn i media
B13: Silslam – mengder, behandlingsløsninger og bruksområder. Forprosjekt.
B14: Klimatilpasningstiltak i VA-sektoren - forprosjekt
B15: Vannforskriftens økonomiske konsekvenser for kommunesektoren og avløpsanleggene
B16: Veiledning for kartlegging av energibruk VA-sektoren
B17: Investeringsbehov i vann- og avløpssektoren

Rapportserie C:

C1: Sårbarhet i vannforsyningen
C2: Stoff for stoff – kilde for kilde. Kvikksølv i avløpsnettet
C3: Samarbeid om økt bruk av avløpsslam på grøntarealer
C4: Effekter av bruk av matavfallskverner på ledningsnett, renseanlegg og avfallsbehandling
C5: Økt sikkerhet og beredskap i vannforsyningen - veiledning
C6: I veien for hverandre - Samordning av rør og kabler i veigrunnen
C7: Forvaltningspraksis ved norsk damsikkerhet

De mest aktuelle rapportene ligger som PDF-filer på www.norskvann.no

- Norsk Vann er en ikke-kommersiell interesseorganisasjon for vann- og avløpssektoren (VA-sektoren). Organisasjonen skal bidra til å oppfylle visjonen om rent vann ved å sikre VA-sektoren funksjonelle rammevilkår og legge til rette for kunnskapsutvikling og kunnskapsdeling.

- Norsk Vann eies av norske kommuner, kommunalt eide VA-selskaper, kommunenes driftsassistanser for VA og noen private andelsvannverk. Norsk Vann representerer ca. 360 kommuner med over 95 % av landets innbyggere. Virksomheten finansieres i hovedsak gjennom kontingenter fra medlemmene.

- Norsk Vann styres av eierne gjennom årsmøtet og av et styre sammensatt av representanter fra eierne.

- I Norsk Vanns prosjektsystem gjennomføres hvert år prosjekter for ca. 8 mill. kroner

- Det er praktiske og aktuelle spørsmål innenfor vann- og avløp som utredes

- Deltakerne foreslår prosjekter, styrer gjennomføringen og får full tilgang til alle resultater

Norsk Vann

Norsk Vann BA, Vangsvegen 143, 2321 Hamar
Tlf: 62 55 30 30 E-post: post@norskvann.no
www.norskvann.no

idetrykk.no