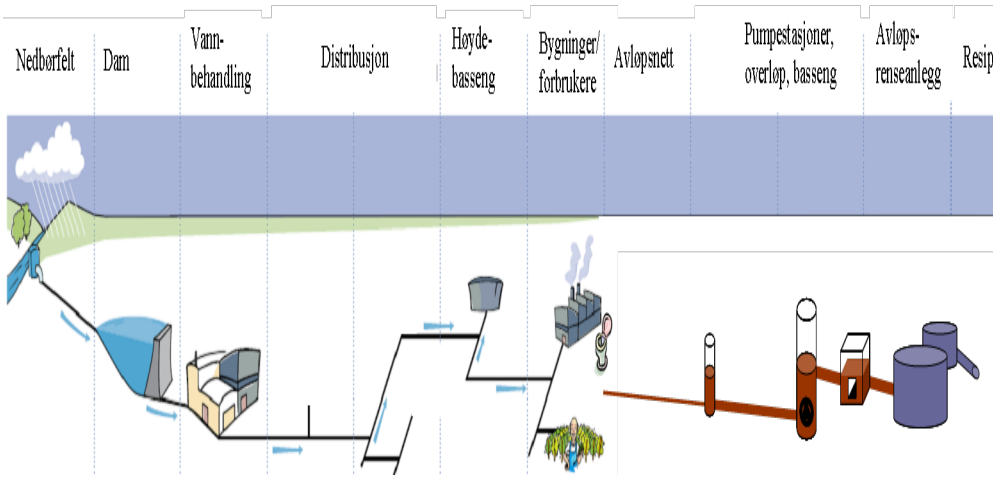
Rapportnummer - Åpen

Rapport

Eksempel på mal for risikovurdering knyttet til informasjonssikkerhet og driftskontrollsystem for vann og avløp

Forfatter(e)
Stig Ole Johnsen
Jon Røstum



SINTEF Teknologi og samfunn
Sikkerhet
2015-07-14

SINTEF Teknologi og samfunn
Postadresse:
Postboks 4760 Sluppen
7465 Trondheim
Sentralbord: 73593000
Telefaks: 73592896
ts@sintef.no
www.sintef.no
Foretaksregister:
NO 948 007 029 MVA

EMNEORD:
Emneord

Rapport

Eksempel på mal for risikovurdering knyttet til informasjonssikkerhet og driftskontrollsystem for vann og avløp

VERSJON
Versjonsnummer

DATO
2015-07-14

FORFATTER(E)
Stig Ole Johnsen og Jon Røstum

OPPDRAGSGIVER(E)
Norsk Vann

OPPDRAGSGIVERS REF.

PROSJEKTNR

ANTALL SIDER OG VEDLEGG:
35+ vedlegg

SAMMENDRAG
Denne rapporten skal være et eksempel på en mal for risikovurdering knyttet til informasjonssikkerhet og driftskontrollsystem for vann og avløp. Rapporten kan være et utgangspunkt når en skal lage sin egen ROS. Rapporten er basert på gjennomførte ROS analyser for DKS/IT systemer i andre vannverk (med kjente dokumenterte sårbarheter som har vært publisert offentlig), og på Norsk Vann Rapport (2013) "Veiledning for sikkerhet av driftskontrollsystemer for VA-systemer".

Målgruppen for ROS-DKS rapporten er de som er ansvarlige for vann og avløp.

Omfanget av en analyse er svært avhengig av størrelse og kritikalitet for vann og avløpsfunksjonen – vi har laget en mal som forsøker å være dekkende for alle, noe som gjør at den dekker mange forskjellige aspekter som ikke alltid er relevant for alle.

UTARBEIDET AV
Stig O. Johnsen

SIGNATUR

KONTROLLERT AV
Kinga Wasilkiewicz

SIGNATUR

GODKJENT AV
Jon Røstum

SIGNATUR

RAPPORTNR	ISBN	GRADERING	GRADERING DENNE SIDE
Rapportnr	ISBN-nummer	Åpen	Åpen

SINTEF

SINTEF

SINTEF

Innholdsfortegnelse

1 Innledning

Denne rapporten skal være et eksempel på en risikovurdering knyttet til informasjonssikkerhet og driftskontrollsystem for vann og avløp, som en skal kunne ta utgangspunkt i lokalt når en skal lage sin egen ROS. Rapporten er basert på gjennomførte ROS analyser for DKS/IT systemer for andre vannverk (med kjente dokumenterte sårbarheter som har vært publisert offentlig), og på Norsk Vann Rapport (2013) "Veiledning for sikkerhet av driftskontrollsystemer for VA-systemer".

Målgruppen for ROS-DKS rapporten er de som er ansvarlige for vann og avløp. Omfanget av en analyse er svært avhengig av størrelse og kritikalitet for vann og avløpsfunksjonen – vi har laget en mal som forsøker å være dekkende for alle, noe som gjør at den dekker mange forskjellige aspekter som ikke alltid er relevant for alle.

Rapporten består av følgende hovedavsnitt:

1	**Innledning**	Definisjoner og begreper Beskrivelse av relevante trusler og uønskede hendelser Beskrivelse av teori og metoder for å lage en ROS analyse Hvordan identifisere og klassifisere uønskede hendelser
2	**Eksempler på risiko og sårbarhetsanalyser**	Objekter som inngår i analysen Deltakere involvert i ROS analysen Sårbarheter og uønskede hendelser opp mot objektene Eksempler på uønskede hendelser, vurderinger og forslag til tiltak Eksempler på risikomatriser / prioriteringer
3	**Eksempler på konklusjoner og anbefalte tiltak**	Oppsummering av konklusjoner og anbefalte tiltak Detaljerte - konklusjoner og anbefalinger
4	**Utvikling av kunnskap og holdninger**	Hvordan utvikle kunnskaper og holdninger
5	**Sentrale standarder og sjekklister som hjelpemidler**	Oversikt over sentrale internasjonale standarder inne området
6	**Referanser og kontakter**	Litteratur referanser og liste over kontaktpersoner/ institusjoner
7	**Vedlegg-I: Sjekklister**	Detaljerte sjekklister for å sikre driftskontrollsystemer innen vann og avløp
8	**Vedlegg-II: Mulige sårbarheter**	Mulige sårbarheter - årsaker til svikt i driftskontrollsystemet, både tilfeldige og utilsiktede feil og bevisst skadeverk
9	**Vedlegg-III: ROS Innholdsliste**	Forslag til innholdsliste for en ROS analyse

1.1 Begreper– informasjonssikkerhet og sikkerhet for driftskontrollsystemer (DKS)

Driftskontrollsystemer (DKS) som brukes til å styre og overvåke VA-systemene (vannbehandlingsanlegg, vanntransport, avløpstransport og avløpsrenseanlegg) er en viktig del av infrastrukturen for vann og avløp.

DKS systemene består av prosessenheter og IT komponenter. Den stadig økende bruken av IT innen drift av VA-systemer har gitt muligheter for bedre overvåkning og styring, noe som har gitt samfunnet gevinster i form av økt effektivisering, pålitelighet og produktivitet. Samtidig har det 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 er tilknyttet kontorstøttesystemer og internett. Dette har introdusert nye farer og trusler. Det er kjent at slike styringssystemer kan manipuleres på ulike måter, noe som medfører at systemene i seg selv kan utgjøre en sikkerhetsrisiko ved at vannforsyningen svikter, den kan forurenses og uønsket avløp kan lede til forurensning.

I det følgende listes sentrale begreper knyttet til dette området:

Informasjonssikkerhet: Beskyttelse av informasjonens konfidensialitet, integritet og tilgjengelighet, fra Nasjonal strategi for informasjonssikkerhet (NSI, 2012).

- **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).

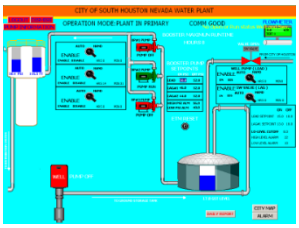
- **Integritet;** det å sikre at informasjonen og metodene/beregningene er nøyaktige og fullstendige. Dette innebærer at uvedkommende ikke kan endre informasjonen eller systemet som behandler informasjonen. Eksempel på tap av integritet er at hackere logger seg på DKS til et vannbehandlingsanlegg og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

1.2 Bakgrunn – Trussel landskap, beskrivelse av relevante uønskede hendelser

Risikoen for at samfunnsviktig infrastruktur, skjermingsverdig informasjon og mennesker blir rammet av spionasje, sabotasje, terror og andre alvorlige handlinger er økende, skriver Nasjonal sikkerhetsmyndighet (NSM 2015) i sin årlige rapport, Risiko 2015. NSM avdekket i 2014 flere alvorlige sårbarheter, blant annet i norsk vannforsyning. Disse sårbarhetene kunne i verste fall gitt uvedkommende mulighet til å lamme vannforsyningen. Til tross for alvorlige sårbarheter og økt risiko, ser NSM at målrettet og systematisk arbeid med forebyggende sikkerhet har en effekt. Flere av sårbarhetene NSM har beskrevet i tidligere rapporter har blitt redusert eller fjernet. I vedlagte tabell har vi dokumentert eksempler på uønskede hendelser i DKS.

Tabell 1.1 Eksempler på uønskede hendelser knyttet til svikt av driftskontrollsystemer (Jaatun og Røstum, 2013).

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 ca. million liter ubehandlet avløpsvann (kloakk) rant ut i nærliggende vassdrag, parker og grøntområder. Se NIST (2008)
Avløpsverket i South Houston - Uvedkommende får tilgang til driftskontrollsystem til VA-verk via internett 	Publikasjon på internett i november 2011 av skjermdump av brukergrensesnitt fra driftskontrollsystemet til vann og avløpsverket i South Houston Nevada. Uvedkommende skal således ha vært i stand til å endre på drifts parametere ved vannverket. Passord for server tilgjengelig via internett etter var "100", som "default" – standard passord. http://pastebin.com/Wx90LLum For å illustrere at også store VA-verk kan være sårbare, nevner vi et ferskt 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 PCer. Testen viste at den innleide hackeren kunne, dersom han ville, ha gjort drikkevannet til flere millioner mennesker udrikkelig
Skallsikring av anlegg Kunne stoppet vanntilførselen med mobilen ** Kunsende, 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
Virus/trojansk hest (Stuxnet) 	Stuxnet, ref. Symantec (2011) 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 utviklet av USA/Israel og inkluderte flere sårbarheter i Windows for å spre seg og/eller infisere DKS programvare.

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 driftskontrollsystem som er tilgjengelig via internett. Dette er et symptom på en utfordring knyttet til sikkerhet og sikring av DKS-ene i VA sektoren.

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 prosesskontroll-systemer, verken i VA-sektoren eller i industrien for øvrig. Det er eksempler på hacking av VA-verk via driftskontrollsystemet (DKS) i USA og automatiserte verktøy gjør det nå enkelt for hackere å lete opp kontrollenheter som er koblet til internett. Det er også enkelt for uvedkommende å skaffe seg informasjon om kritiske deler av et DKS via internett. Standard passord ("default") for enkelte systemer kan finnes via internett, og manualer og videoer for hvordan de ulike DKS virker kan også lastes ned. Dette gjør det mulig for ikke-eksperter å tilegne seg kunnskap om eventuelle sårbarheter ved de enkelte DKS.

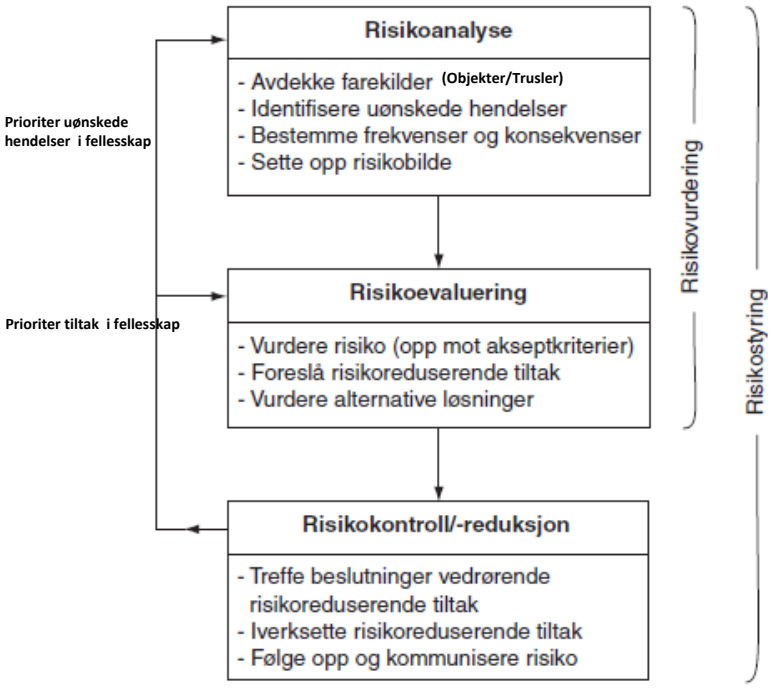
En undersøkelse i regi av Svenskt Vatten, (Johansson 2010) pekte også på lite fokus på informasjonssikkerhet knyttet til DKS systemer. Dette gjaldt både svake IT- løsninger i selve DKS systemet, men også lite fokus på IT- sikkerhet i VA-verket selv. Vanlige ROS-analyser av VA-sektoren har oftest fokusert på prosesstekniske problemstillinger. Siden kunnskap om IT-systemer som regel representerer et fremmed fag-område 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 IT 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 administrasjons-nett, som igjen gjerne er koblet mot Internett. Den økende bruken av IT, sammen med økt bruk av hyllevare og økt sammenkobling mot andre nett, gjør at sårbarheten når det gjelder IT-trusler er større enn før. Av den grunn er det viktig at VA-verkene har stor oppmerksomhet på å beskytte driftskontrollsystemene.

1.3 Teori, metoder og arbeidsmåter

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) – og et systematisk informasjonssikkerhetsarbeid. I figur 1.1 er det vist et eksempel på en standard risikovurdering og risikostyring. Aktivitetene står beskrevet i denne rapporten. For å sikre forståelse, eierskap og engasjement anbefales det at prioritering av uønskede hendelser og prioriteringer av tiltak gjøres i fellesskap med de ansatte/involverte som vist i vedlagte figur.

Det er viktig at en basert på ROS-analyser i hvert VA-verk identifiserer de mest kritiske komponenter av VA-systemet 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.



Figur 1-1: Risikovurdering og risikostyring

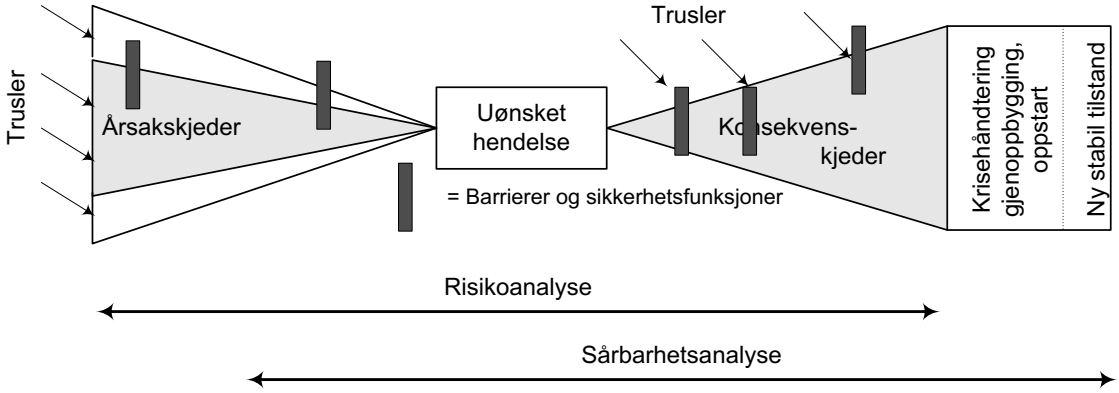
1.3.1 Risikovurdering - Risiko og sårbarhetsanalyse

I en risiko og sårbarhetsanalyse (ROS-analyse) 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:

a. Hva er kritiske komponenter og hva kan gå galt knyttet til driftskontrollsystem i VA? Kritikaliteten må vurderes ut i fra begrepene *konfidensialitet*, *integritet* og *tilgjengelighet*
b. Hvilke barrierer/tiltak kan redusere sannsynligheten for at noe går galt?
c. Hvilke barrierer/tiltak kan redusere konsekvensene hvis noe går galt?

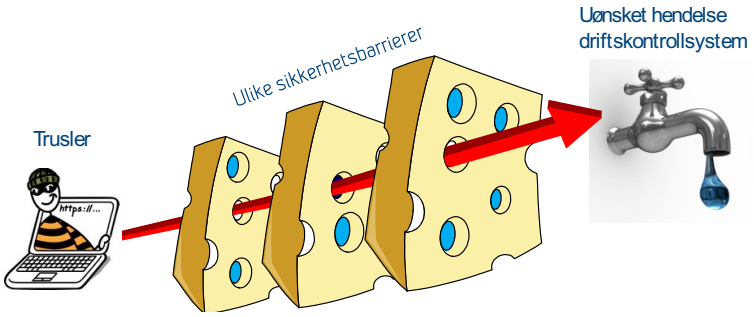
En risiko- og sårbarhetsanalyse må dokumentere kritiske komponenter, trusler, risikoer og tiltak for gjenvinning som forsøkt illustrert i figur 1-2. Man har ulike trusler som kan forårsake en uønsket hendelse. En slik uønsket hendelse kan igjen ha uønskede konsekvenser. Ulike former for barrierer og 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: 1-2: Illustrasjon av en risiko- og sårbarhetsanalyse med trusler (farer), uønskede hendelser, årsaks- og konsekvenskjeder, barrierer og sikkerhetsfunksjoner

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

- **Bygge inn sikkerhet**. Sørge for at en bygger robuste systemer som er testet og sertifisert slik at de kan håndtere kjente angrep, bygge inn sikkerhet i bredde (dvs. inkludere tekniske, menneskelige og organisatoriske tiltak) og dybde (med forsvar i dybde av de mest kritiske objektene).
- Implementere **tekniske tiltak/planer** (f.eks. etablere skallsikring av anlegg, segmentering av datanett), fastsettelse av tekniske målepunkter/styringspunkter og oppfølging av disse (f.eks. logging av avbruddsdata for kommunikasjon for å fange opp trender)
- **Menneskelige faktorer som kursing/trening**. Dekker tiltak både i forkant av hendelser for å unngå at hendelsene oppstår og trening for å håndtere hendelser i etterkant f.eks. i forbindelse med beredskapsøvelser.
- Etablere **organisatoriske driftsrutiner** (f.eks. etablere rutiner for periodisk skifte av personlig passord, gjennomføre logging av kritiske operasjoner).



Figur 1-3"Sveitserost modell" som illustrasjon på flere sikkerhetsbarrierer for driftskontrollsystem

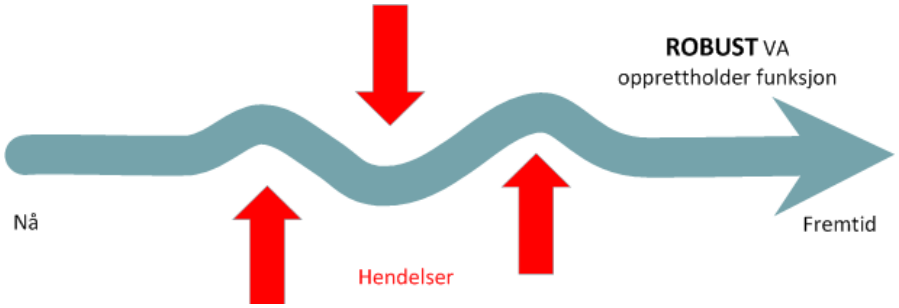
For å illustrere at flere sikkerhetsbarrierer må svikte samtidig for at en uønsket hendelse skal opptre, brukes ofte "sveitserostmodellen, hvor hver enkelt av sikkerhetsbarrierene kan ha svakheter/"hull". Eksempler på sikkerhetsbarrierer er mekanismer som hindrer at en hacker klarer å koble seg på driftskontrollsystemet 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 tekniske/fysiske, menneskelige og organisatoriske. Ulykker skjer når alle hullene i de ulike sikkerhetsbarrierene (osteskiver) ligger på rekke.

1.3.2 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 hendelser. Dette er illustrert i figuren 1-4 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 helt ute av funksjon. Dette gjelder både overfor eksterne (hacking, virus) og interne svakheter som VA-verket selv styrer med. Det betyr f.eks. at vi har reservesystemer eller manuelle systemer som kan tre i verk ved et problem.
- Ved bortfall av driftskontrollsystemet skal en fortsatt kunne levere tilfredsstillende VA-tjenester. Konsekvensene av bortfall av driftskontrollsystemet skal altså være så små som mulig.



Figur 1-4: Illustrasjon av et robust vann- og avløpssystem som opprettholder sin kjernefunksjon selv om det utsettes for uønskede hendelser

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. 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.

1.4 Hvordan identifisere og klassifisere uønskede hendelser

I USA har en samlet inn hendelser og angrep på IT og industrielle styringssystemer, i en egen kommersiell database, www.risidata.com, som har samlet inn data fra 2001, kalt "Industrial Security Incidents Database (ISID)". Det som er erfaring fra innsamlede hendelser er følgende:

- **20% bevisste angrep**
  - fra eksterne hackere (9,4%) eller
  - fra innsida -ansatte, konsulenter. – (10,6%)
- **80% ubevisste hendelser** som skyldes
  - feil i komponenter eller programvare (38,4%),
  - "Generell Malware" (30,4%), dvs generelle virusangrep
  - Menneskelige feilhandlinger (11,2%).

Analysene fra denne databasen dokumenterer at trusselbildet er sammensatt, slik at det er viktig med tiltak både i bredde (ivareta flere trusler) og i dybde (dvs beskytte kritiske områder med flere tiltak.). Den største årsaken er feil i komponenter eller programvare (38,4%), og det er derfor viktig med tiltak for å styrke dette området, f.eks. ved å øke testingen via f.eks. sertifisering.

For å identifisere uønskede hendelser, bør man hente inn data fra tidligere uønskede hendelser (f.eks. i dialog med industrien, og via interne intervju) og gjennomføre en strukturert idémyldringsprosess med viktige ressurspersoner. Denne består vanligvis av tre faser eller trinn som beskrevet i det følgende. I hvert av trinnene er det viktig å ha fellesmøter hvor deltakerne kan bidra med å prioritere de viktigste verdiene/objektene:

A1. Identifisere og prioritere verdier/objekter i systemene; hva er det vi skal beskytte? Identifisere aktører/interessenter; hvem er involvert eller kan ha interesse?

A2. Identifisere og prioritere de viktigste uønskede hendelser; hva kan gå galt, evt. hva ville en angriper ha lyst og mulighet til å gjøre? (I vedlegg II har vi laget en liste over relevante sårbarheter.) For å få frem kritikaliteten av komponentene kan en diskutere konsekvenser av at objektene:
   a. Stopper i en periode (1 time, 1 dag, 1 uke) eller fungerer ikke som planlagt (ukontrollerbart)
   b. Prioriteringen gjøres på basis av å vurdere sannsynlighet(S) og Konsekvens (K)

A3. Foreslå og prioriter risikoreduserende tiltak

Risiko fastsettes ut ifra sannsynlighet og konsekvens for en uønsket hendelse. Sannsynlighet og konsekvens er i dette prosjektet kategorisert i henhold til definerte felles kriterier som er beskrevet av Mattilsynet (2006) som er tilpasset for også å dekke avløp

Tabell 1.2 Beskrivelse av sannsynligheter

S-NIVÅ	KRITERIER
S1: Liten sannsynlighet	a: Hendelsen er ukjent i bransjen b: Faglig skjønn tilsier at hendelsen ikke helt kan utelukkes c: Trusselvurdering tilsier at hendelsen er lite sannsynlig
S2: Middels sannsynlighet	a: Bransjen kjenner til at hendelsen har inntruffet de siste 5 år b: Faglig skjønn og føre-var hensyn tilsier at det er riktig å ta høyde for at hendelsen kan oppstå i vannverket de neste 10-50 år c: Trusselvurdering tilsier at hendelsen er middels sannsynlig
S3: Stor sannsynlighet	a: Det er kjent i bransjen at hendelsen forekommer årlig b: Vannverket har selv opplevd enkeltstående tilfeller, eller hendelsen har nesten inntruffet c: Faglig skjønn og føre-var hensyn tilsier at hendelsen kan oppstå i vannverket i løpet av de neste 1-10 år d: Trusselvurdering tilsier at hendelsen har stor sannsynlighet
S4: Svært stor sannsynlighet	a: Hendelsen forekommer fra tid til annen i vannverket b: Trusselvurdering tilsier at hendelsen har svært stor sannsynlighet

Tabell 1.3 Beskrivelse av konsekvensklasser

K-NIVÅ	KRITERIER
K1: Liten konsekvens	a: Liv & helse/kvalitet: Kvalitet påvirkes ubetydelig, gjeldende krav overholdes b: Kvantitet/kapasitet: Ubetydelig påvirkning c: Omdømme: Omdømme ikke truet d: økonomi: økonomisk tap mindre enn 5 % av årlig kostnader e: Miljø: Mindre miljøskade. Utbedret innen noen dager
K2: Middels konsekvens	a: Liv & helse/kvalitet: Kortvarig, mindre brudd på gjeldende krav (vann) /1 skade som trenger medisinsk hjelp (avløp) b: Kvantitet/kapasitet: Kortvarig (timer) svikt til enkelte områder c: Omdømme: Omdømme belastet d: Økonomi: økonomisk tap 5-10 % av årlig kostnader e: Miljø: middels miljøskade. Utbedret innen noen uker.
K3: Stor konsekvens	a: Liv & helse/kvalitet: Brudd på gjeldende krav, ulempe for helse (vann)/flere skader som trenger medisinsk /sykehus (avløp) b: Kvantitet/kapasitet: Langvarig svikt (dager) til enkelte områder c: Omdømme: Omdømme kortvarig tapt/skadet d: Økonomi: økonomisk tap 10-20 % av årlig kostnader e: Miljø: Stor miljøskade. Utbedret innen noen måneder.
K4: Svært stor konsekvens	a: Liv & helse/kvalitet: Alvorlig brudd på gjeldende krav, fare for liv og helse, drikkevannsforskriftens § 18 trer i kraft (vann) / flere skader som trenger medisinsk /sykehus minst en alvorlig skadet (avløp) b: Kvantitet/kapasitet: Langvarig svikt som rammer flertallet av abonnentene c: Omdømme: Omdømme langvarig tapt/skadet d: økonomi: økonomisk tap større enn 20 % av årlig kostnader e: Miljø: Svært stor miljøskade som det vil ta år å lege

Kombinasjonen av sannsynligheter og konsekvensklasser for uønskede hendelser gir et uttrykk for risikonivået. Ved å lage en matrise med sannsynligheter og konsekvenser får man en risikomatrise som gir en grafisk fremstilling av risikonivået. En risikomatrise er derfor sammensatt av sannsynlighet for og konsekvenser av ulike hendelser. Sannsynlighet og konsekvens av en hendelse gir til sammen et uttrykk for risikoen som hendelsen representerer. Risikomatrisen kan deles inn i tre hovedområder:

- Rødt: Risikoreduserende tiltak skal iverksettes. (dvs. høy sannsynlighet / høy konsekvens)
- Gult: Risikoreduserende tiltak skal vurderes på basis av akseptkriterier i bransjen, vanlig er at en følger et prinsipp som heter ALARP som er en forkortelse av "As Low As Reasonably Practicable", og innebærer at risiko reduseres så langt praktisk gjennomførbart. Basert på vannverkets egne vurderinger, faktakunnskap og solid faglig skjønn.
- Grønt: Risikoreduserende tiltak er ikke nødvendig. (dvs lav sannsynlighet / lav konsekvens)

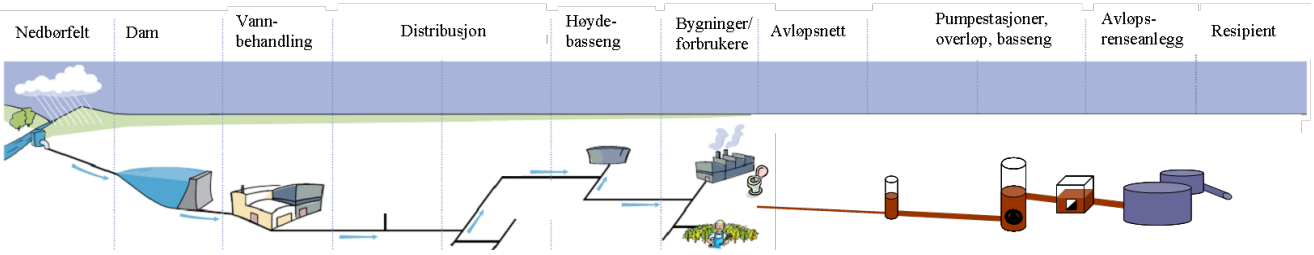
Akseptkriterier uttrykker en øvre grense for hva man vurderer å være et akseptabelt risikonivå for visse kategorier av uønskede hendelser. Krav i helse-, miljø- og sikkerhetslovgivningen utgjør en viktig ramme for denne øvre grensen, og det er dermed ikke adgang til å sette til side spesifikke krav i helse-, miljø- og sikkerhetslovgivningen med henvisning til vurdert risiko. For risiko som er høyere enn akseptabelt nivå, skal det iverksettes tiltak for å bringe sikkerheten innenfor akseptkriteriene.

2 Eksempler på risiko og sårbarhetsanalyser for å styrke robustheten

2.1 Objekter som inngår i analysen

I det følgende beskriver vi konteksten(vann og avløp) og objekter (fysiske objekter, tekniske styringssystemer, organisasjon og mennesker) som må inngå i en ROS-analyse. Figur 2.1 viser hele VA-kjeden fra nedbørfelt via vannbehandling og distribusjonsnett, til avløpsnett og videre til avløpsrenseanlegg. For hvert objekt bør man derfor dokumentere DKS systemene som er kritiske, f.eks. pumper med styringssystemer. I tillegg til systemer som er viktige innen VA-infrastrukturen, er man avhengig av IT-systemer for samband og kommunikasjon. Vi har i vedlagte figur skissert objekter som bør inngå i en kritikalitetsvurdering, dvs. for hvert objekt bør en også gå gjennom teknisk utstyr og tilhørende DKS/IT systemer som kontrollerer objektet.

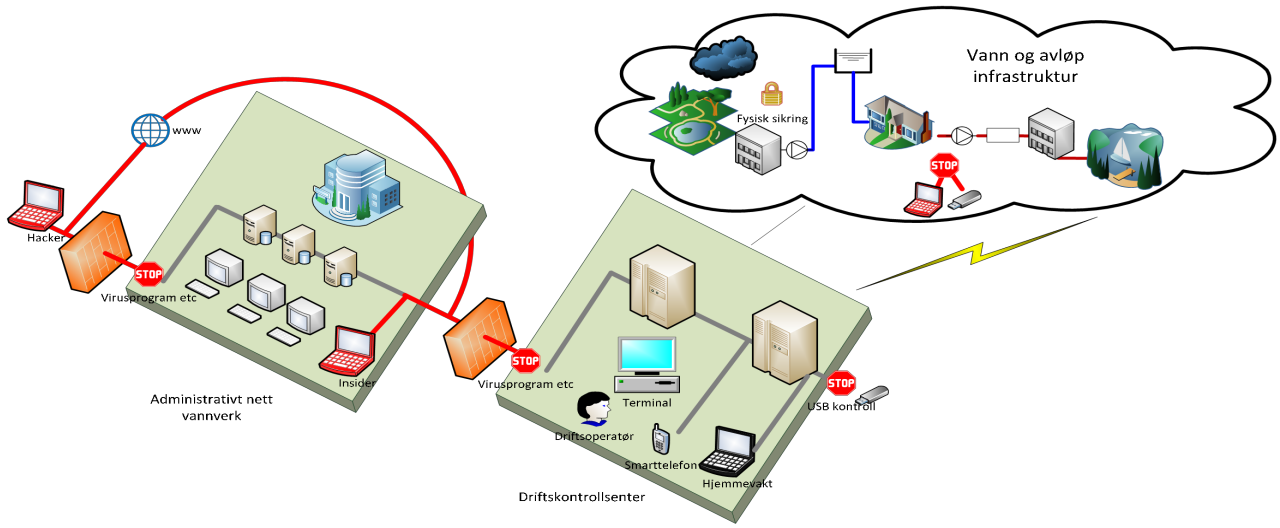
Objekter:	1-Dam	2-Vannbeh.	3 Vannledningsnett	4-Avløpsnett	5-Avløpsrensing
	6- Felles teknisk infrastruktur : Datanett (administrativt nett, teknisk nett), koblinger til Internett, Driftskontrollsenter				



Figur 2.1: Kontekst: Elementer i vann og avløp fra nedbørfelt til resipient (mottaker)

For å styre denne prosessen er det etablert PLS-systemer i vann og avløp infrastruktur, datanett, driftskontrollsenter og administrative nett, som vist i figur 2.2. Disse tekniske komponentene er en del av objektene som inngår i analysen. I tillegg har vi de organisasjonene som har ansvaret, vannverk, tekniske underleverandører, IT avdelinger og den enkelte ansatt med sine kunnskaper og holdninger.

Tekniske Objekter:	6A: Nett (Admin.,teknisk DKS)	6B: Driftskontrollsenter	6C: Admin. systemer	6D:Strøm, kjøling



Figur 2.2: Felles tekniske objekter.

2.1.1 Deltakere i ROS analysen

Det er viktig at ROS analysen gjennomføres i et samarbeid mellom ledelsen, sikkerhetseksperter, IT fagfolk, DKS fagfolk, drift og evt. eksterne eksperter/ leverandører som kan ha ansvaret for deler av infrastrukturen. Både for å sikre at de forskjellige fagavdelingene kan gi innspill, men også for å sikre at det etableres god kommunikasjon, dialog og enighet om analyse/sårbarheter, evaluering/vurderinger og prioritering av tiltak. Deltakere i arbeidet bør dokumenteres for sporbarhet, men er også ønskelig ut fra senere avklaringer eller oppfølginger. Vanligvis er dette også et ønske fra tilsynsmyndighetene at deltakelsen er dokumentert.

Tabell: Deltakere i ROS analysene (risikoanalyse, risikoevaluering, prioriteringer)

Deltakere	Ansvar	Intervju	Møtedeltakelse		
			Analyse	Evaluering	Tiltak
NN	Ledelse	DD/MM	DD/MM	DD/MM	DD/MM
NN	IT				
NN	Sikkerhet/Sikring				
NN	DKS				
NN	Drift				
NN	Eksperter/ Leverandører				

2.2 Sårbarheter og uønskede hendelser opp mot objektene

I det følgende har vi listet opp eksempler på objekter og sårbarheter for vann og avløp knyttet til DKS og IKT. Sårbarhetene dekker hele MOT (Menneske, Organisasjon og Teknologi).

Tabell 2-1: Objekter, sårbarheter og elementer som inngår i en kritikalitetsvurdering

Objekter (Ansvar)	Tekniske sårbarheter for DKS systemene	Organisatoriske sårbarheter	Menneskelige sårbarheter
Objekter med tilhørende DKS systemer	DKS Styringssystemer – fysisk sikring, IT adgangskontroller, robusthet mot virus - Siste "patcher" er lagt inn, feilvarsling, logging, Segmentert nett, Sertifiserte komponenter i nettet, gode alarmer for kritiske komponenter	Ledelsens fokus på sikkerhet, og oppfølging av sikkerheten. Ansvar (fra tidlig anskaffelse, bygging til drift), vaktordninger (med kompetente ressurser), beredskap og dokumenterte beredskapsplaner, rutiner for gjennomgang av logger, Rutiner for å administrere brukere – brukerid, passord, dokumentasjon av nettet og systemene	Kunnskap om sårbarheter, trening, holdninger (sett informasjonssikkerhet på agendaen), risikokommunikasjon, kommunikasjon om hendelser
1-Kilde/dam med tilhørende DKS			
2-Vannbehandling			
3 – Vannledningsnett inkl pumper, ventiler høydebasseng			
4-Avløpsnett inkl pumper			
5-Avløpsrenseanlegg			
6A: Nett og brannmurer (Admin.,teknisk DKS) med fjernstyringstilgang, linjesikkerhet			
6B: Driftskontrollsenter			
6C: Admin. systemer - f.eks. Geodatasystemer			
6D:Strømforsyning/ UPS, Kjøling m/reserve, driftssentral			

For å identifisere uønskede hendelser, bør man som sagt hente inn data fra tidligere uønskede hendelser. i dialog med NSM, industrien, og via interne intervju/spørreundersøkelser. I vedlegg I har vi listet opp aktuelle spørsmål (mulige sårbarheter i bransjen) som kan benyttes som et utgangspunkt for arbeidet. I vedlegg II er det listet opp kjente sårbarheter i bransjen og forslag til tiltak.

Et viktig arbeidsredskap er å gjennomføre strukturert idémyldringsprosess med viktige ressurspersoner, for både å identifisere sårbarheter (som kan utnyttes/bli en uønsket hendelse) og for å kunne prioritere uønskede hendelser og tiltak. For å få frem kritikaliteten av komponentene kan en diskutere konsekvenser av at objektene stopper i en periode 1 time, 1 dag, 1 uke eller Ikke fungerer som planlagt (ukontrollerbart)

For hver uønsket hendelse vil man anslå en grov sannsynlighet for hendelsen (S) og deretter identifisere en konsekvens (K) basert på klassifiseringene fra Mattilsynet (2006). Prioriteringen gjøres på basis av å vurdere sannsynlighet(S) og konsekvens (K) plassert i en risikomatrise – deretter vil mulige risikovurderende tiltak identifiseres og eventuelt implementeres.

I det følgende har vi dokumentert:

- Eksempel og skjematikk for å dokumentere uønskede hendelser
- Eksempler på risikomatrise og bakgrunn for prioriteringer
- Eksempler på konklusjoner og anbefalinger

2.3 Eksempler på dokumentasjon av uønskede hendelser, vurderinger og forslag til anbefalte tiltak

I det følgende har vi listet opp eksempler på uønskede hendelser, risikovurderinger (S-sannsynlighet og K-konsekvens) samt forslag til tiltak med angivelse av prioritet og ansvarlig (med måldato).

Fare/U-uønsket hendelse (Med årsak)	K	S	T-Tiltak (Kostnad)	Prioritet	Ansvarlig (Måldato)
Langvarig strømbrudd hvor en ikke har nødstrøm som leder til svikt i datanett, IT-systemer, både adm og styringssystem.	K3	S2	Nødstrømsaggregat på kritiske komponenter		
Hacking/ Inntrenging i nettet via hjemmevakt-PC. Uvedkommende tar over styring av kritiske VA-funksjoner.[1]	K4	S2	Restriksjoner på hva en kan gjøre fra hjemmevaktordning. Vurdere om kritiske PCer skal ha ekstra beskyttelse. Passord		
Virusangrep mot vannbehandlingsanlegg f.eks via infeksjon via hjemmevakt-PC.	K3	S3	Stenge for muligheten av at kritiske DKS PC kan ha DKS-tilgang og nettilgang samtidig	.	
Lav kjennskap til datasikkerhet, manglende kjent regelverk for sikkerhet leder til dårlig sikkerhet og uønskede hendelser via kunder og underleverandører	K3	S3	Systematisk fokus på sikkerhet via kursing, etablering av regelverk internt og eksternt, jamnlig trening på uønskede hendelser		
Dårlige rutiner for rapportering av hendelser	K3	S2	Uønskede hendelser rapporteres og deles via kurs og beredskapsøvelser		
En har ikke trent på beredskapsøvelser hvor IKT er involvert	K3	S2	Årlige beredskapsøvelser etableres		
Applikasjoner på har dårlig datasikkerhet og kan bidra til økt sårbarheter	K3	S3	Datasikkerhet etableres som krav ved anskaffelse, testing av tilfredsstillende sikkerhet gjennomføres før systemene tas i bruk		
Ufullstendige oversikt over brukere av systemene, med uklare ansvarsforhold, og dårlige sikkerhetsrutiner	K2	S3	Skriftlig policy etableres, ansvaret for oppfølging legges til en ansvarshavende		
Innbrudd, tyveri eller sabotasje av sentralt drift (Switcher/ Rutere)	K3	S4	Fysisk sikring av sentrale komponenter		
Brann (som leder til at sentrale DKS systemer stopper/ blir ødelagt)	K2	S4			
Feilkonfigurering av sentral brannmurer som leder til følgefeil	K2	S3			
Generell virusinfeksjon som leder til ustabilitet i nettet	K3	S3			
Målrettet virusinfeksjon som legges inn for å avlytte (hente data)	K2	S3			

[1] For illustrasjon har en for en slik villed handling angitt sannsynlighet og konsekvens og ikke anbefalt fremgangsmåte som beskrevet iNorsk Vann rapport: Sikkerhetsstyring for vannbransjen med bruk av *sårbarhet, verdi og trussel*. (http://www.norskvann.no/10-nyheter/1026-ny-rapport-sikkerhetsstyring-for-vannbransjen)

2.4 Eksempler på risikomatriser / prioriteringer

Rødt: Risikoreduserende tiltak skal iverksettes.
Gult: Risikoreduserende tiltak skal vurderes.
Grønt: Risikoreduserende tiltak er ikke nødvendig.

Tabell 2 2: Risikomatrise

		Konsekvens			
		K1: Liten konsekvens	**K2: Middels konsekvens**	**K3: Stor konsekvens**	**K4: Svært stor konsekvens**
Sannsynlighet	**S4: Svært stor sannsynlighet**				
	S3: Stor sannsynlighet		• Ufullstendige oversikt over brukere av systemene • Feilkonfigurering av sentral brannmure	• Virusangrep mot kritisk DKS vannbehandling • Lav kjennskap til datasikkerhet • Applikasjoner på har dårlig datasikkerhet • Generell virusinfeksjon	
	S2: Middels sannsynlighet			• Strømbrudd langvarig • Dårlige rutiner for rapportering av hendelser • Manglende beredskapsøvelser knyttet til IKT • Innbrudd, tyveri eller sabotasje • Målrettet virusinfeksjon som legges inn for å avlytte	• Hacking av kritiske PCer via hjemmevakts PC • Brann serverrom, DKS
	S1: Liten sannsynlighet				

SINTEF

PROSJEKTNR	RAPPORTNR	VERSJON
Prosjektnummer	Rapportnummer	Versjonsnummer

SINTEF

3 Eksempler på konklusjoner og anbefalte tiltak

Nedenstående eksempler på konklusjoner og anbefalte tiltak fra en ROS analyse. Funnene er generiske, dvs. de har relevans for andre vannverk og andre bransjer. Vi har valgt å innlede med en oppsummering, før den detaljerte opplistingen for å kunne presentere de viktigste resultatene på en kortfattet form og for å gi en kontekst for detaljene.

3.1 Oppsummering - konklusjoner og anbefalte tiltak

Risikovurderingen for DKS/IT viser at det er flere sikkerhetsutfordringer å ta tak i. En viktig sårbarhet er at informasjonssikkerhet i stor nok grad ikke er på agendaen. Det kommuniseres lite, det finnes for lite tydelige regler og rutiner, og informasjonssikkerhetsaspekter kommer sent inn i prosjekter. Mye fungerer likevel godt i den daglige driften, men beskyttelsene vil være lett å omgå for både egne ansatte og uvedkommende som ønsker å påføre skade på vannverket eller kundene/brukerne.

En bør særlig vurdere å gjennomføre følgende risikoreduserende tiltak knyttet til IKT:

- IKT må forankres sterkere hos ledelsen og integreres tettere med alle prosjekter
- Gjennomgang av hvilke VA-funksjoner som er mest kritiske og sørge for at IT-systemene knyttet opp mot disse er sikret i henhold til ønsket sikkerhetsnivå. Dette inkluderer også kommunikasjon og strømforsyning. Dette krever en detaljert analyse i samarbeid med leverandører av telekommunikasjon og strømforsyning. Dette tiltaket adresserer en rekke av de identifiserte uønskede hendelsene.
- Vannverket oppfordres til å samle inn historiske data for å analysere linjesikkerhet/avbruddslogg kommunikasjon basert på sine egne data.
- Etablere sonedeling av kommunikasjonsnettet og skille prosesskontrollsystemer fra administrative systemer og Internett i så stor grad som mulig

3.2 Detaljerte - konklusjoner og anbefalinger

I dette kapitlet beskrives ulike sårbarheter og trusler for systemer, som er avdekket gjennom prosjektmøter. Til hver beskrivelse følger en anbefaling (skrevet i kursiv) som en kan ta med seg i det videre arbeidet med sikkerhet. Kapitlet er strukturert i henhold til tre hovedtema; organisatoriske forhold, fysisk sikring og IT-drift.

3.2.1 Organisatoriske forhold

IKT-sikkerhetsreglement

Sentralt er det et IKT-sikkerhetsreglement som gjelder for alle underliggende enheter, men opplevelsen internt er at ingen leser dette, ingen bruker dette aktivt, og nyansatte signerer ikke på det når de begynner. Endringer kan dessuten inntreffe uten at de ansatte blir informert.

Anbefalte tiltak: *Ledelsen bør ta stilling til i hvilken grad informasjonssikkerhet er viktig for vannverket, og kontinuerlig kommunisere dette til de ansatte gjennom ulike kanaler.*

Beredskapsplaner og håndtering av IKT-sikkerhetshendelser

Det finnes rutiner knyttet til beredskap rundt IKT-sikkerhetsbrudd, men det står svært lite om dette i beredskapshåndboken for vannverket.

Anbefalte tiltak: *For å unngå at man er avhengig av kunnskap hos enkeltpersoner, bør eksisterende rutiner for beredskap rundt IT-sikkerhetsbrudd dokumenteres i beredskapsplanene.*

Det er lite kommunikasjon internt rundt IT-sikkerhetshendelser. Når slikt inntreffer, blir det tatt tak i og ordnet opp slik at driften stabiliseres som normalt, og så er man ferdige med hendelsen. Det er ingen fast informasjonsflyt, evaluering eller læring i etterkant.
Anbefalte tiltak: *En kunne med fordel ha vært mer åpen om IT-sikkerhetshendelser internt. Dette bidrar til opplæring og bevisstgjøring av ansatte, samt til å sette informasjonssikkerhet på agendaen.*

Utydelig ansvar for IKT i vannverket.
Ansvaret for IKT er uklart. Er det IT-avdelingen i kommunen som har overordnet ansvar eller er det vannverkseier?
Anbefalte tiltak: *Vannverkseier må foreta en avklaring med IKT avdelingen i kommunen.*

3.2.2 Fysisk sikring

Fysisk sikring av IKT-utstyr
Kart over ledningsnettet, ligger lagret på PCer, det uheldig om denne informasjonen kommer på avveie gjennom at en PC blir stjålet eller på andre måter blir borte.
Anbefalte tiltak: *En bør ha tydelige regler for oppbevaring av IT-utstyr som inneholder informasjon om VA-ledningsnettet ihht anbefalinger gjort av Norsk Vann om at ledningsnettet ikke skal ligge tilgjengelig på nett.*

Adgangskontroll utestasjoner
Adgangskontroll til utestasjonene er under utvikling og man har opplevd noen problemer. De fleste utestasjonene har følgende løsning:

- sensor i dørlås og/eller bevegelsesdetektor
- driftspersonell har egen nøkkel, andre kan bruke utlånsnøkler
- uautorisert inngang trigger innbruddsalarm til vaktsentral

Anbefalte tiltak: *Vannverket børe foreta en gjennomgang av adgangskontroll ved utestasjoner.*

Dokumentasjon av nettverk
Dokumentasjonen som er gjort av sambandene pr dato er ikke tilfredsstillende. Nettverkstopologi er dokumentert, men svitsjer og nettverkskabling ikke merket. Det mangler kryssreferanser mellom tegninger, og referanser mot elektrodokumentasjonen. Datablad på utstyr er ikke tilgjengelig på stasjonenes sluttdokumentasjonsmappe. Ofte er vitale kommunikasjonskomponenter ikke sikret med backup-batteri. Manglende oversikt gjør at slike mangler er vanskelig å oppdage.

Anbefalte tiltak: *Det er behov for å etablere et prosjekt som går på bedre merking av kabler etc..*

3.2.3 IKT-drift

Sonedeling – kommunikasjonsnett
Nettet er ikke inndelt i soner, dermed kan alle nå alt når de er på nettsegmentet. Man kan bruke samme PC til både drift og administrasjon. Det er tilgangsstyring på driftsapplikasjonene, slik at de ikke kan benyttes av andre enn de som er gitt eksplisitt tillatelse. Det å skille prosesskontroll fra administrative systemer er

allerede gjennomført i VA-miljø i en del norske kommuner. Da har man ikke Internett-tilgang fra prosess-kontrollsystemene, og man har ikke anledning til å utføre kommunal saksbehandling på maskiner som brukes til prosesskontroll.

Anbefalte tiltak: *Vannverket bør på det sterkeste vurdere innføring av sonedeling i sitt nett. Fordelen med en slik inndeling i soner vil være at en kan seksjonere ut en sone dersom noe inntreffer og fortsatt drifte resten av nettet. Dessuten vil man lettere kunne gjennomføre strengere tilgangsstyring dersom dette er eller blir et behov.*

Passordrutiner
Man må endre sitt passord på administrative systemer hver 3. måned. Kravene til dette passordet er at det er minst seks tegn, og man kan ikke gjenbruke de fem forrige passordene sine. Det er ingen krav om store og små tegn og tall. Det er ikke implementert "single-sign-on", men mange ansatte bruker samme passord på alle jobb-systemene, slik at når man må endre det ene, endrer man samtidig de øvrige.
Anbefalte tiltak: *Single sign-on er å anbefale, men dette er opp til kommunen å gjennomføre. Fordelen med single sign-on er at de ansatte kan forholde seg til alle jobbsystemene med kun ett passord, og det er mulig å ha gode sikkerhetsmekanismer rundt dette passordet; tydelige krav og gode lagrings- og krypteringsmekanismer.*

I fjernkontrollsystemene finnes det fellesbrukere hvor passordet deles mellom flere ansatte. Dette vanskeliggjør sporing av endringer, da man ikke kan vite hvem som faktisk har vært innlogget på tidspunkt man ønsker å undersøke nærmere. Dessuten medfører det ofte lavere sikkerhet rundt passordet, det skrives ned på lapper rundt tastaturet eller andre steder.
Anbefalte tiltak: *Så langt det er praktisk mulig, anbefales det å ha unike brukere med egne passord i alle systemer, nettopp for å øke sikkerheten rundt hvert enkelt passord og for å sikre sporbarhet.*

Hjemmevaktordning
PC som har driftsapplikasjonene installert, tas med hjem og kan i prinsippet brukes av andre i husholdningen. Tilgangen hjemmefra skjer via VPN-forbindelse til en terminalserver. Gjennom bruk hjemme er det en generell fare for malware-infeksjoner.

Anbefalte tiltak: *Valgt ordning for vaktordningen er en avveining mellom kostnader, konfidensialitet og tilgjengelighet. Ved å ha hjemmevaktordning sikrer en høy tilgjengelighet og lave kostnader. Utfordringen er derimot og også sikre konfidensialiteten til systemet. Det er viktig at en jevnlig foretar vurdering knyttet til disse forholdene..*

Mangel på varsel ved svikt i alarmsystem
Det oppleves av og til svikt i forbindelse med alarmer som går på spesielle installasjoner. Ofte er det problemer som går på ansvarsforhold og grenseoppganger slik at disse alarmene ikke blir håndtert.
Anbefalte tiltak: *Det bør vurderes om alarmsystemet kan implementeres på en mer intelligent måte og det er behov for organisatoriske avklaringer og tydeliggjøring av rutiner for å hindre denne type feil.*

Forslag til metode for å analysere linjesikkerhet til viktige utestasjoner
I https://ics-cert.us-cert.gov/content/overview-cyber-vulnerabilities gis det en oversikt over sårbarheter i

forskjellige typer nett. I det følgende foreslås en praktisk fremgangsmåte for å identifisere kritiske utestasjoner som har behov for god linjesikkerhet/kommunikasjon og hvordan dette kan analyseres.

1. **Lage oversikt over de viktigste/mest kritiske utestasjonene.** Hvilke krav skal en stille til de enkelte utestasjoner/brukersted? En del utestasjoner vil ha en viktigere funksjon enn andre og dette må gjenspeiles i kravene til oppetid. Viktige utestasjoner kan for eksempel være noen av høydebassengene, alle vannbehandlingsanlegg og noen av de større vannpumpestasjoner.
2. **Analysere feilhistorikk mht. kommunikasjon til utestasjoner**. Dette kan gjøres ved å ta utgangspunkt i alarmsignaler. Leverandør av alarmsystem og driftsovervåkningssystem bør etablere slike datasystemer som kan lagre historiske sviktdata for de *ulike kommunikasjonskomponenter* (hvor stort bidrag fra henholdsvis PLS, bredbånd, telekomleverandør, driftssentral etc.).
3. **Analysere de enkelte kritiske utestasjoner** i lys av faktisk oppsett og vurdere sviktdata for de enkelte komponenter. Basert på en slik analyse kan tiltak for å forbedre linjesikkerheten iverksettes.

Anbefalte tiltak: *En må foreta en gjennomgang av hvilke VA-funksjoner/stasjoner som er mest kritiske mht. linjesikkerhet/kommunikasjon og sørge for at IT-systemene knyttet opp mot disse er sikret i henhold til ønsket risikonivå.*

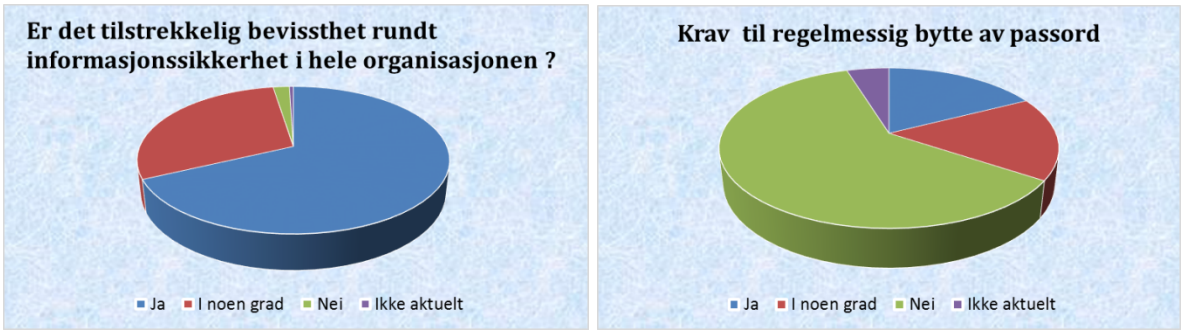
SINTEF

4 Utvikling av kunnskap og holdninger

I NOU 2012: 14 Rapport fra 22. juli-kommisjonen, står det som et viktig funn:
1. Kommisjonens viktigste anbefaling er at ledere på alle nivåer i forvaltningen systematisk arbeider med å styrke sine egne og organisasjonenes grunnleggende holdninger og kultur knyttet til

- *risikoerkjennelse,*
- *gjennomføringsevne,*
- *samhandling,*
- *IKT-utnyttelse, og*
- *resultatorientert lederskap.*

I en fersk undersøkelse utført av Mattilsynet i 2015[2] ble det sendt ut et spørreskjema til omlag 500 vannverk basert på sjekklisten utarbeidet i Norsk Vann rapport 195/2013. Figur 4.1 viser to resultater fra undersøkelsen som illustrerer det manglende fokus på informasjonssikkerhet i vannbransjen. På spørsmålet om "*Er det tilstrekkelig bevissthet rundt informasjonssikkerhet i hele organisasjonen?*" svarer 67 % "Ja" og 30 % "i noen grad". Dvs vannbransjen i Norge synes rimelig fornøyd med eget ambisjonsnivå og bevissthet vedrørende informasjonssikkerhet. Når det derimot kommer til mer konkrete spørsmål slik som: "*Er det krav til regelmessig bytte av alle passord?*" svarer 61 % "Nei". Dette viser at det er lite sammenfall mellom svarene på de ulike spørsmål og det er grunn til å tro at mange vannverk ikke har full forståelse av de spørsmålene som stilles. NSM sin vurdering av resultatene fra Mattilsynets undersøkelse er at Vannbransjen i Norge ikke skjønner at de ikke skjønner informasjonssikkerhet.



Figur 4.1: Eksempler på svar fra Mattilsynets spørreundersøkelse i 2015 til norske vannverk knyttet til informasjonssikkerhet.

Det kan derfor være verdt å jobbe med holdninger og kultur, ved å kartlegge og diskutere dette med ledelsen. I den forbindelse har SINTEF utviklet et verktøy som heter CheckIT i samarbeid med NSM, JBV, Telenor, Rikstrygdeverket, Statens forvaltningstjeneste og NTNU se Johnsen et al (2007) og:
www.sintef.no/prosjekter/sintef-teknologi-og-samfunn/2005/sjekkit/

CheckIT verktøyet kan brukes systematisk for å diskutere og utvikle sikkerhetskulturen som ofatter kunnskaper og holdninger om sikkerhet.

[2] Presentasjon av Mattilsynet på TEKNA sin konferanse "Samfunnssikkerhet og vannbransjen, 21-22 april 2015.

SINTEF

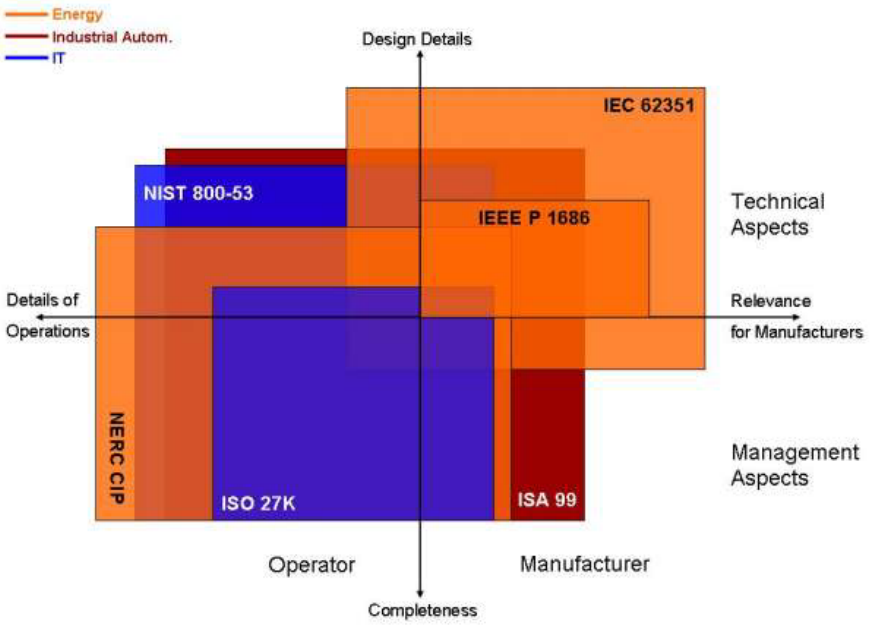
5 Sentrale standarder og sjekklister som hjelpemidler

Når det gjelder regelverk og bransjestandarder er det flere sentrale standarder knyttet til "safety" og "security" av IT og prosessutstyr som er sentrale, som: IEC 61508, ANSI/ISA-62443, ISO/IEC 27001 og IEEE Standard 802.11. Standardene er kort beskrevet i Tabell 5-1, og innbyrdes dekningsgrad er beskrevet i Figur 5-2.

Tabell 5-1: Relevante internasjonale standarder for IT og DKS systemer

Internasjonal standard	Vurdering
ANSI/ISA-62443 – (2007) Security for Industrial Automation and Control Systems (Også benevnt ISA99).	Sikkerhetsstandard for DKS og IT, fokus på "Safety" og "Security". (Begynner å bli brukt av industrien). Dekningsgraden er vurdert av ESCORT (2011).
The ISASecure certification based on ANSI/ISA-62443 – standards	Sertifisering og testing av komponenter bør gjøres for at systemene skal bli mer robuste. Enten sertifisering via ISASecure Embedded Device Security Assurance Certification – ref. www.isasecure.org, eller via Achilles (f.eks. fra www.wurldtech.com). I tillegg kan en nevne IDART "Read Team" testing fra SANDIA, som sjekker kvaliteten av forsvar og barrierer I tidligfase, ref IDART (2014) (NSM har rutiner for sertifisering, via organet SERTIT- det har vært lite brukt.)
ISO/IEC 27001:2013 – Information technology – Security techniques –Information security management systems – Requirements.	Sikkerhetsstandard for IT, fokus på "Information security". Ut fra økt bruk av IT til styring av DKS, bør ISO 27001 være en sentral referanse.
IEC 61508 (2010) Functional safety of electrical/ electronic/ programmable electronic safety-related systems.	Sikkerhetsstandard for prosessutstyr, fokus på "Safety", er i utstrakt bruk. Bl.a. I OLF070 – Norwegian oil and gas application of IEC 61508 and IEC 61511 in the Norwegian petroleum industry
IEEE Standard 802.11 wireless local network specifications	Ut fra sikkerhetshensyn bør en ta med IEEE 802.11i: Enhanced security (2004) and IEEE 802.11w: Protected Management Frames (2009)
God praksis for datasikkerhet basert på: *"20 Critical Security Controls"* fra www.sans.org/critical-security-controls/	Sjekkliste som dokumenterer beste praksis for datasikkerhet.
EU Directive 2008/114/EC (iverksatt 2012 i Norge) EPCIP-direktivet gjelder for grenseoverskridende infrastruktur og for infrastruktur i enkeltland. Den gjelder for vann og avløp.	Forskrift om objektsikkerhet (1. januar 2011). Forskriften skal sikre at objekter som må beskyttes av hensyn til rikets sikkerhet og vitale nasjonale interesser blir identifisert og beskyttet. Objektene skal klassifiseres som VIKTIG, KRITISK eller MEGET KRITISK, avhengig av skadepotensial. Den som eier eller råder over objekter skal aktivt ta del i identifisering og klassifisering av egne skjermingsverdige objekter. Av andre relevante dokumenter kan nevnes U.S. National Infrastructure Protection Plan - NIPP (2009), som har forslag til hvordan objekter kan sikres på forsvarlig måte..

I Figur 5-2, har vi skissert hvordan et utvalg av standarder fra IT, industriell automasjon og energisektoren er posisjonert i forhold til operatører og leverandører, og hvordan de dekker tekniske aspekter eller styringsaspekter.



Figur 5-2: Dekningsgrad for de forskjellige standardene (Ref ESCORT 2011)

Ut fra figuren er det ANSI/ISA-62443 (ISA 99) som har den bredeste dekningen og som ivaretar forhold knyttet til industriell automasjon.

Norsk vann har utformet en sjekkliste som kan brukes for å sjekke ut sikkerhet knyttet til DKS innen VA. Sjekklisten er også utformet som et enkelt regneark, og kan lastes ned fra www.norskvann.no., den ligger også som vedlegg-I i denne rapporten. Av andre relevante sjekklister/god praksis kan nevnes:

- NSM (2014) Ti viktige tiltak mot dataangrep (Oppdater versjon via www.nsm.stat.no)
- NERC (2007) Top 10 Vulnerabilities Of Control Systems And Their Associated Mitigations – 2007
- The Center for Internet Security(2015) "Critical Security Controls" via www.counciloncybersecurity.org/critical-controls/ beste praksis fra USA

Det er også laget veiledninger for sikring av DKS systemer som kan være nyttig å sette seg inn I – verdt å nevne er:

- Luiijf, E. (2008) "SCADA Security Good Practices for the Drinking Water Sector," TNO TNO-DV 2008 C096; som beskriver sårbarheter, god praksisi og relevante kilder for å sikre vannanlegg

- Dokument som gir bakgrunn for sårbarheter I DKS systemer NIST SP 800-82 "Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Con¬trol Systems Security" - Se http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf

SINTEF

6 Referanser/ Kilder og Organisasjoner (kontaktpersoner)

ANSI/ISA-62443-1-1 (99.01.01)-2007 Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models

Escort (2011) "Escorts – Security of control and realtime systems – R&D and standardization Road Map, final Deliverable 3.2".
EU Directive 2008/114/EC , COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008, on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

IDART - The Information Design Assurance Red Team (IDART) ref http://idart.sandia.gov/, from 2014
ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements.
IEC 61508 (2010). "Functional safety of electrical/electronic/programmable electronic safety-related systems", IEC.

Johansson E., (2010) "Kartläggning av SCADA-säkerhet inom svensk dricksvattenförsörjning," SvensktVatten C29 120

Johnsen, S.O., Hansen, C.W., Line, M.B., Nordby, Y., Rich, E. and Qian, Y.: "CheckIT - A Program to Measure and Improve Information Security and Safety Culture". Included in International Journal of Performability Engineering (ISSN 0973-1318) on Risk and Safety Management. Paper 15 - pp. 174-186, Volume 3, Number 1, January 2007.
Luiijf, E. (2008) "SCADA Security Good Practices for the Drinking Water Sector," TNO TNO-DV 2008 C096.

Mattilsynet (2006) "Økt sikkerhet og beredskap i vannforsyningen – Veiledning" fra Mai 2006

Norsk Vann Rapport (2013) "Veiledning for sikkerhet av driftskontrollsystemer for VA-systemer"

NSI (2012) – "Nasjonal strategi for informasjonssikkerhet" fra Justis- og beredskapsminster Grete Faremo; Forsvarsminister Anne-Grete Strøm-Erichsen; Samferdselsminister Marit Arnstad; Fornyings-, administrasjons- og kirkeminister Rigmor Aasrud.

NSM (2015) - Nasjonal sikkerhetsmyndighet "Risiko 2015".

NSM (2014) *Ti viktige tiltak mot dataangrep* (Oppdater versjon via www.nsm.stat.no)

- Noe mer detaljert: The Center for Internet Security(2015) "*Critical Security Controls*" via www.counciloncybersecurity.org/critical-controls/
- NERC (2007) *Top 10 Vulnerabilities Of Control Systems And Their Associated Mitigations* – 2007, North American Electric Reliability Council, Control Systems Security Working Group, U.S. Department of Energy, National SCADA Test Bed Program, at energy.gov/sites/prod/files/oeprod/DocumentsandMedia/NERC_2007_Top_10.pdf

NIST (2008) National Institute of Technology and Standards -Computer Security Resource Center (CSRC) *"Malicious Control System Cyber Security Attack Case Study–Maroochy Water Services, Australia"*
http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf
NIST SP 800-82 "Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security" - Se http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf

Objektsikkerhetsforskriften - Forskrift om objektsikkerhet (2010) lovdata.no/dokument/SF/forskrift/2010-10-22-1362

Rausand M., Utne I. B.,(2009) "Risikoanalyse. Teori og metoder". Trondheim: Tapir Akademisk Forlag 2009.

Symantec. (2011). W32.Stuxnet Dossier, retrieved 2011-03-01
www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

Sikkerhetsloven (1998) - Lov om forebyggende sikkerhetstjeneste, Forsvarsdepartementet, 1998. Available: www.lovdata.no/all/nl-19980320-010.html

SINTEF

7 Vedlegg-I : Sjekkliste for sikre driftskontrollsystemer innen vann og avløp

Denne sjekklisten er hentet fra Norsk Vann Rapport (2013) "Veiledning for sikkerhet av driftskontrollsystemer for VA-systemer". En annen veiledning som ansees som nyttig for vannverk er NSM sin veiledning knyttet til "Sikring av industrielle automatiserte kontrollsystemer" som fås ved å kontakte NSM.

1) Er informasjonssikkerhet i driftskontrollsystemer godt nok forankret hos ledelsen i VA-verket?
2) Er det bevissthet rundt informasjonssikkerhet i hele organisasjonen?
3) Har alle personlig brukernavn og passord ved pålogging av DKS?
4) Er alle standardpassord fjernet?
5) Er det krav til tilstrekkelig styrke på passord?
6) Er det krav til regelmessig bytte av passord?
7) Kreves det 2-faktor autentisering ved ekstern tilgang til DKS (VPN, terminalserver)?
8) 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?
   a) Vurdering av de som har intern / ekstern tilgang til systemer. (Vandelsattest / taushetsplikt)
9) Er det spesifisert ulike nivåer på tilgangsrettigheter (innsyn, endring)?
10) Gjennomgås tilgangsrettigheter årlig for å sikre at alle tilgangsrettigheter er korrekte og på riktig nivå?
11) Er det gjennomført en ROS-analyse som dekker hjemmevaktordning?
12) Er det egne PC, nettbrett etc. som bare brukes til drift og vakt?
13) 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)?
14) Er det vurdert skille, eventuelt sikkerhetsbarrierer mellom administrative og DKS nett?
15) Er det vurdert skille, eventuelt sikkerhetsbarrierer mellom internett og DKS?
16) Har VA-verket vurdert kritikaliteten/viktigheten av de ulike utestasjoner/VA-anlegg?
17) Er det egne DKS-nett for henholdsvis vann og avløp (sonedeling)?
18) Er det foretatt *geografisk* sonedeling av DKS nett?
19) Er det mekanismer som begrenser muligheten til å få tilgang til andre deler av DKS fra hvilken som helst utestasjon?
20) Finnes det et system for registrering av hendelser og avvik i virksomheten?
21) Finnes det et eget system for systematisk registrering av hendelser og avvik (svikt) for DKS?
   a) Evt. er det hensiktsmessig å registrere DKS hendelser og avvik i det generelle avvikssystemet
22) Finnes det nedskrevne rutiner for håndtering av hendelser og avvik i DKS?
23) Er det lett for uvedkommende å få innsyn i opplysninger om geografisk plassering av VA-infrastruktur?
24) Har en sikret redundans av kritiske systemer/komponenter (to servere, kommunikasjon, strømforsyning, datarom)?
25) Er det noen anlegg som ikke kan driftes i manuell modus når man mister kontakt med utestasjonene (vannbehandlingsanlegg)
26) Finnes det avtaler for informasjonssikkerhet mot eksterne driftsleverandører?
27) Finnes det systemer for inntrengningsdeteksjon (IDS)?
28) Finnes det rutiner/mekanismer for viruskontroll mot DKS?
29) Finnes det rutiner for oppdatering/patching av systemer i DKS?
30) Har VA-verket gjennomført en analyse av DKS koblinger mot andre system (Internett, administrative system etc) som kan utgjøre en fare?
   a) Vurdering av sikkerhet i de forskjellige nettverk / radiosamband
31) Dekker beredskapsplanen også DKS hendelser?

32) Er beredskapsplanen blitt oppdatert siste år?
33) Er det tilstrekkelig skallsikring av VA-infrastruktur slik at det ikke er for enkelt å få fysisk adgang til infrastrukturen?
34) Står den fysiske sikringen av anleggene i forhold til viktigheten av VA-anleggene?
35) Er det gode rutiner for å sikre tilstrekkelig opplæring og videreutdanning av personell i informasjonssikkerhet?
36) Gjennomføres det periodiske ROS analyser i VA-verket som i tilstrekkelig grad også fokuserer på informasjonssikkerhet og DKS?
37) Har VA-verkets beredskapsøvelse også inkludert IKT/DKS hendelser?
38) Har VA-verket beredskap og forberedte tiltak for alternativ drift av VA-systemet ved svikt i hele eller deler av driftskontrollsystemet?
39) Har VA-verket tilstrekkelig egen kompetanse innen informasjonssikkerhet og DKS, eller er de helt avhengig av leverandører og konsulenter?
40) Har VA-verket en avtale om full backup av konfigurasjon av DKS?
41) Har VA-verket tilstrekkelig faglig bestillerkompetanse ved nyanskaffelser av DKS?
42) Har man satt krav til oppe-tid for DKS?
43) Er alle systemløsningene og beskrivelsene av DKS godt dokumentert?
    a) Systemdokumentasjon
    b) nettverksdiagram
    c) strømforsyningsdiagram
    d) datautveksling mot eksterne enheter
        i) andre DKS
        ii) verdier for vedlikeholdssystem (FDV)
        iii) rapportering,
        iv) VPN
        v) …
44) Foretas det periodisk oppdatering av system / DKS dokumentasjon?
45) 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.

SINTEF

8 Vedlegg-II: Mulige sårbarheter - årsaker til svikt i driftskontrollsystemet

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 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 8-1: 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 sikker-hetsfunksjoner/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 også 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 byg-ges inn (brannmur, tilgangskontroll, overvåking)
DKS er fysisk koblet sammen med internett	Internett-tilgang fra driftskontrollsystem er praktisk for operatør for å være på internett når det er liten aktivitet på drifts-kontrollsenteret, 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 tilkoblingsmuligheter og USB-porter til drifts-kontrollsystem.	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	Enkelte typer nettsteder er mer utsatte enn andre, men det finnes også	• Egne PC for hjemmevakt uten annen programvare

Sårbarhet	Beskrivelse	Avbøtende tiltak
i forbindelse med hjemmevakt kan lett bli infisert av skadelig kode dersom infiserte eller ondartede nettsteder besøkes.	eksempler på uskyldige nettsteder som via banner-reklamer har spredt virus. Dersom hjemmevakts PC også brukes av familiens andre medlemmer i forbindelse med nettsurfing og andre aktiviteter, er det store muligheter for infisering av PC. En smittet PC kan deretter smitte DKS fra innsiden når den kobles til nettverket når en kommer tilbake til jobb.	• 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 organisasjonen	Pulverisering av ansvar. Uklar rollefordeling mellom Ikt avdeling i kommunen og vannverkseier.	• Viktig at IT sikkerhet er satt på dagorden i organisasjonen og at ledelsen prioriterer dette. Dette inkluderer implementering av gode rutiner for IT-sikkerhet/ sikkerhetspolicy i organisasjonen som definerer roller og ansvar.
Mangelfull kunnskap om IT-sikkerhet i organisasjonen	Trusselbildet endrer seg fort innen IT-sikkerhet som en følge av rask utvikling. Stort behov for kontinuerlig etter-utdanning. 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 bevissthetstiltak
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
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 ute-stasjoner (vegskap/uteskap, pumpestasjoner, eller høydebasseng).	• Bedre fysisk sikring av vegskap/uteskap • Sonedeling av nett

Tabell 8-2 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 8-2: 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)

8.1 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, strømbrudd, feil med systemet eller backup-systemer typiske tilfeldige og utilsiktede feil. Spesielt kan avhengigheten av nøkkelpersonell, og mulig mangel på kompetanse være en sårbarhet.

8.1.1 Teknisk svikt.

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

8.1.2 Naturgitt skade.

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

8.1.3 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 å alene benytte teknologiske sikkerhetsbarrierer (som viruskontroll og redundant kommunikasjon), men også basere seg på organisatoriske forhold (etablere prosedyrer, sjekklister, kvalitetssikringsrutiner, godkjenningsordninger, arbeidskontroll) 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 konsulenter 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 8.2).

8.2 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.

8.2.1 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.

8.2.2 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[3] 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

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

SINTEF

9 Vedlegg-III: Forslag til innholdsliste for ROS analysen

I det følgende er det laget et forslag for innholdsliste til en "Risikovurdering knyttet til informasjonssikkerhet og driftskontrollsystem for vann og avløp ", som en skal kunne ta utgangspunkt i når en skal lage sin egen ROS.

Omfanget av en analyse er svært avhengig av størrelse og kritikalitet for vann og avløpsfunksjonen –malen forsøker å være dekkende for alle. Det gjør at den dekker mange forskjellige aspekter som ikke alltid er relevant for alle. Innholdslisten må derfor tilpasses lokale forhold.

Rapporten består av følgende hovedavsnitt:

1	**Innledning**	Definisjoner og begreper Beskrivelse av relevante trusler og uønskede hendelser Beskrivelse av metoder for å lage en ROS analyse Hvordan en har identifisert og klassifisert uønskede hendelser
2	**Risiko og sårbarhetsanalyser**	Objekter som inngår i analysen Deltakere involvert i ROS analysen Sårbarheter og uønskede hendelser opp mot objektene Uønskede hendelser, vurderinger og forslag til tiltak Risikomatriser / prioriteringer
3	**Konklusjoner og anbefalte tiltak**	Oppsummering av konklusjoner og anbefalte tiltak Detaljerte - konklusjoner og anbefalinger
4	**Utvikling av kunnskap og holdninger**	Hvordan skal vi utvikle kunnskaper og holdninger i vår organisasjon
5	**Standarder og sjekklister som brukes**	Oversikt over standarder og sjekklister vi bruker
6	**Referanser og kontakter**	Referanser
7	**Vedlegg-I: Sjekklister/ Intervju**	Utfylte sjekklister/ Oppsummering av intervju