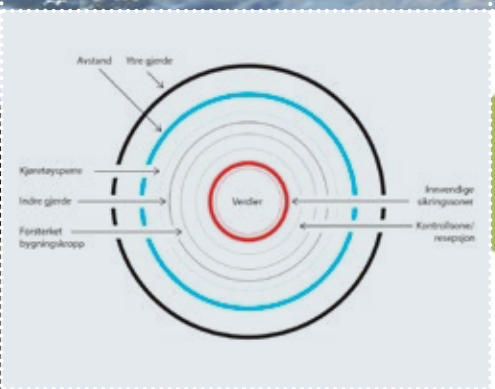
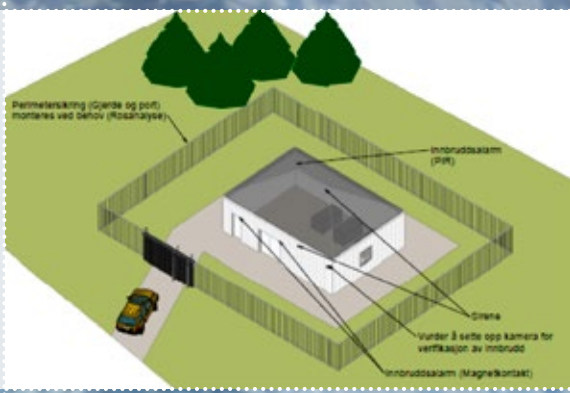
Norsk Vann

Rapport

229 | 2017

Sikring av vannforsyning mot tilsiktede uønskede hendelser





Norsk Vann

Norsk Vann Rapport

Det utgis tre 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

Prosjektresultatene fra Norsk Vann Rapport (serie A og B) kan fritt benyttes internt i egen organisasjon. Når prosjektresultatene benyttes i skriftlig materiale, må kilde oppgis. Videresalg/ formidling av resultatene utover dette er kun tillatt etter skriftlig avtale med Norsk Vann BA.

Norsk Vanns rapporter utarbeides i samspill mellom rådgiver, styringsgruppe og referansegruppe for prosjektet og er ikke behandlet i Norsk Vanns styrende organer. Norsk Vann har ikke ansvar for feil eller ufullstendigheter som måtte forekomme i rapporten og kan ikke stilles økonomisk eller på annen måte til ansvar for problemer som måtte oppstå som følge av bruk av rapporten.

Norsk Vann

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

Norsk Vann Rapport

Ekstrakt
I Norsk Vann prosjektrapport 229 gis anbefalinger om hvordan vannforsyningsanlegg effektivt kan sikres mot tilsiktede uønskede hendelser. Bakgrunnen for prosjektet er usikkerhet om hvordan vannverkene kan gjøre trusselvurderinger og hvilke sikringstiltak som bør gjennomføres for å møte truslene. Ny drikkevannsforskrift fra 1.1.2017 stiller krav om at alle deler av vannforsyningen er tilstrekkelig fysisk sikret. I veilederen beskrives hva som er viktig å sikre, hvordan vannverkene kan vurdere trusselbildet og hvordan de bør sikres. Veilederen gir en rekke konkrete råd om fysisk sikring av ulike deler av vannforsyningen.

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

Rapportens tittel
Sikring av vannforsyning mot tilsiktede uønskede hendelser

Forfattere
Leif Riis og Anniken Hareide, Forsvarsbygg

Rapportnummer: 229/2017

ISBN 978-82-414-0403-0 (trykt utgave)
ISBN 978-82-414-0404-7 (elektronisk utg.)
ISSN 1504-9884 (trykt utgave)
ISSN 1890-8802 (elektronisk utg.)

Emneord, norsk
Vannforsyning, fysisk sikring, tilsiktede uønskede hendelser

Emneord, engelsk
Water supply, safeguarding, securing, premeditated and malicious acts

Forord

Gjennom intervjuer med vannverk i Norsk Vann prosjektet «Sikkerhetsstyring i vannbransjen» kom det frem at vannverkene i mindre grad hadde gjennomført tiltak mot tilsiktede uønskede hendelser. Det var usikkerhet knyttet både til trusselvurdering og til valg av nivå for sikringstiltak. Ny drikkevannsforskrift fra 1.1.2017 stiller imidlertid krav om at alle deler av vannforsyningen er tilstrekkelig fysisk sikret. Vurderinger av trusselnivå skal gjøres lokalt av vannverkseier i samarbeid med lokalt politi. Imidlertid viser det seg at dette er vanskelige fordi det i begrenset grad er mulig å få støtte til trusselvurderingene, og følgelig er det vanskelig å fastsette riktig nivå på sikringstiltakene.

> «Formålet med rapporten er å gi vannverkene en god veiledning i valg av nivå for sikringstiltak»

Målsettingen med dette prosjektet er å utarbeide en veiledning som skal gi vannverkseier en beskrivelse av hvordan fastsette trusselnivå og lage en konkret veileder for hvordan fysisk sikre vannverk utfra aktuelt trusselnivå. Målsettingen er langt på veg oppfylt i denne rapporten, men ettersom dette er relativt upløyd mark i vannsektoren er det behov for å samle erfaringer, beskrive beste praksis og oppdatere veiledningen.

Norsk Vann vil gjerne ha forslag til forbedringer av rapporten fra vannverk som har prøvd anbefalingene og/eller gjort egne erfaringer. Utfra tilbakemeldinger vil rappporten revideres når vi ser at det er behov for dette.

Rapporten er skrevet av Anniken Hareide og Leif Riis i Forsvarsbygg. Styringsgruppen for prosjektet har bestått av:

- Leif Terje Øvernes, IVAR
- Trond Løver, Vestfold Vann
- Thomas Brændvik, Narvik Vann
- Sigurd Grande, Oslo kommune VAV
- Odd Yngvar Lian, Kristiansand kommune

En referanse gruppe bestående av følgende personer har kommet med verdifulle innspill og synspunkter underveis og bidratt til økt presisjon og kvalitet på rapporten:

- Øystein Haavardstein, IVAR
- Carl C Cibbern, Vitek
- Ole Moskaug, Ringerike kommune
- Roger Jarnstedt, Ancistrus
- Tor Håkonsen, Norconsult
- Arne Espeland, Mattilsynet
- Petter Lindgren, NRV
- Stig Ove Olsen, NSM
- Eirik Dalsbø Lohne, Tromsø kommune
- Mai Riise, Hias
- Anna Walde, Bergen kommune
- Kjetil Tveitan, HOD
- Mats Frank, Sande kommune

Ancistrus AS har bidratt med verdifulle erfaringer og bilder til rapporten.
Engasjert rådgiver Einar Melheim har vært prosjektleder, mens avdelingsleder Kjetil Furuberg har vært fagansvarlig hos Norsk Vann.

Anbefalingene i rapporten er drøftet i styringsgruppen, men ikke behandlet i Norsk Vanns styrende organer. Norsk Vann takker alle som har bidratt til rapportens innhold. Forhåpentlig vil den motivere mange vannverk til å starte arbeidet med fysisk sikring.

Hamar, desember 2017
Einar Melheim, Norsk Vann

Sammendrag

Den nye drikkevannsforskriften, som trådte i kraft 1. januar 2017, stiller skjerpede krav til vannverkenes beredskap og forebyggende sikkerhetsarbeid. Med det trusselbildet som Norge står ovenfor i dag innebærer dette at man må sikre seg mot tilsiktede uønskede handlinger som terror, etterretningvirksomhet, sabotasje, hærverk og annen kriminalitet. Mange av dagens vannbehandlingsanlegg og distribusjonssystemer ble bygget for flere tiår siden, da både trusselsituasjonen og kravene fra myndighetene ikke var så tydelige som de er i dag. I mange tilfeller vil disse vannbehandlingsanleggene og distribusjonssystemene derfor hverken tilfredsstille dagens forskriftskrav eller ha mulighet til å håndtere trusler som anleggene kan blir utsatt for. Formålet med denne veilederen er følgelig å gi vannverkene mer oppdatert kunnskap om hvordan man effektivt kan sikre bygg og anlegg mot tilsiktede uønskede handlinger, slik at de kan gjennomføre sikringstiltak som vil kunne forebygge, forhindre og redusere konsekvensene av uønskede hendelser.

Veilederen er delt inn i tre hoveddeler. Med unntak av innledningskapittelet er alle kapitteloverskriftene formulert som spørsmål for å gi lesere en god forståelse for hva hvert kapittel tar sikte på å svare på. Under følger et kort sammendrag av de tre hoveddelene:

Hvorfor må vannforsyningen sikres?

Norges drikkevannsforsyning er utpekt av Direktorat for samfunnssikkerhet og beredskap (DSB) som en kritisk samfunnsfunksjon. Det vises til at drikkevannsforsyningen er kritisk fordi tilgangen til vann er en grunnleggende fysiologisk forutsetning for alt liv og viktig også av hygieniske og sanitære årsaker. Svikt i drikkevannsforsyningen vil også kunne få konsekvenser for samfunnets evne til å ivareta en rekke andre kritiske funksjoner som matproduksjon, helsevesen og industri.

Drikkevannsforskriften stiller følgelig krav til vannverkseierne med hensyn til kvalitet, mengde og leveringssikkerhet. Forskriftens § 10 om forebyggende sikkerhet stiller krav om at vannbehandlingsanlegget og alle relevante deler av distribusjonssystemet skal ha tilstrekkelig fysisk sikring. Hva som menes med «tilstrekkelig fysisk sikring» utdypes imidlertid ikke. I denne veilederen tolkes tilstrekkelig fysisk sikring som tilstrekkelig helhetlig sikring, bestående av fysisk og elektronisk sikring samt administrative og organisatoriske sikringstiltak (menneskelige sikringstiltak).

Hva skal vi sikre og hvem skal vi sikres oss mot?
Et av de mest grunnleggende spørsmålene som skal stilles når man setter i gang med sikrings- og sikkerhetsarbeid er hvilke verdier man har, og hva som skal sikres. Før vannverkene går i gang med sikringsarbeidet må det derfor gjennomføres en verdivurdering av det aktuelle vannforsyningssystemet. I verdivurderingen må alle verdier som understøtter forsyningssystemets drift og leveranse identifiseres og rangeres etter viktighet. Verdiene rangeres etter hvilke konsekvenser det vil ha for systemet dersom denne verdien skulle falle bort. Denne verdivurderingen danner utgangspunkt for hva som skal sikres og hvor godt de skal sikres.

Den norske drikkevannsforsyningen kan rammes av en rekke ulike uønskede tilsiktede handlinger innen trusselkategoriene terror, sabotasje, etterretning og annen kriminalitet. Hendelsene kan omfatte alt fra bombetrusler fremsatt over telefon, hærverk og enkelt innbrudd, angrep som involverer bomber og sprengstoff til andre former for fysisk sabotasje, dataangrep, samt ulike former for forgiftning med kjemiske, biologiske eller radiologiske substanser. Det er mulig å tenke seg anslag mot høydebasseng, pumpestasjoner, vannbehandlingsanlegg, hovedledningsnettet eller tilførselen til spesifikke bygninger. Angrep kan utføres av alt fra pøbler og psykisk ustabile personer, utro tjenere eller tidligere ansatte som av ulike grunner ønsker å ramme vannverket, til aktører med terrortrening eller militærbakgrunn.

Det er viktig å bemerket at dette kapittelet ikke er ment som en offisiell trusselvurdering for alle norske vannverk, men som et grunnlagsdokument som vannverkene kan ta i bruk i utarbeidelsen av egne mer spesifikke trusselvurderinger. Dette følger blant annet av at det trusselbildet som de ulike vannverkene står ovenfor vil endre seg etter forhold som for eksempel størrelse og beliggenhet, så vel som hvem eller hva det aktuelle vannverket forsyner. Det er derfor avgjørende at hvert enkelt vannverk foretar en egen trusselvurdering for å kartlegge relevante trusler.

Hvordan sikrer vi oss? (Prinsipper og praksis)

Sikringstiltak som implementeres bør fremstå som så gode og effektive at en som angriper vil vurdere muligheten for å lykkes med et angrep som lav. Sikringstiltak vil da ha en forebyggende og avskrekkende effekt. Dersom en eller flere angripere likevel forsøker seg, må angrepet detekteres raskt slik at mottiltak kan iverksettes for å stoppe angrepet og begrense skadevirkningene. For å oppnå en slik sikring bør prinsippet om en helhetlig sikring følges og det bør etableres et sikringssystem som består av en kombinasjon av barrierer, deteksjon, verifikasjon, reaksjon og gjenoppretting. For at de etablerte sikringstiltakene skal ha ønsket effekt er det også helt avgjørende at det etableres en god sikkerhetskultur i virksomheten. Det er mennesket som skal utføre virksomhetens tekniske og organisatoriske sikkerhetstiltak. Dårlig sikkerhetskultur vil derfor raskt kunne redusere effekten av kostbare fysiske og elektroniske sikringstiltak ved at de motarbeides av ansatte som ikke forstår hvorfor, eller er uenig i at de er etablert.

Det finnes i dag flere tusen vannverk i Norge. Disse vannverkene strekker seg fra å være små, private vannverk som kun forsyner noen få abbonenter til å være store offentlig vannverk som forsyner over 100 000 abonnenter. Det er ikke hensiktsmessig å beskrive en sikring som skal være dekkende for alle disse vannforsyningssystemene. Dette skyldes store variasjoner i både design og byggemåte, så vel som at ulike vannforsyningssystem og ulike deler av forsyningen kan stå ovenfor ulike trusler avhengig av for eksempel sårbarhet, størrelse, beliggenhet og kritiske abonnenter. Både grunnsikringen og eventuell tilleggssikring for hvert enkelt anlegg må derfor utarbeides på grunnlag av en egen risiko- og sårbarhetsanalyse (ROS). I ROS-analysen vurderes hvilke verdier en virksomhet har, hvor sårbare disse verdiene er ovenfor et sett med utvalgte trusselscenarier, risikobildet og hvordan man skal håndtere risiko. En slik analyse vil gi vannverkene en oversikt over risikobildet hvert enkelt anlegg står ovenfor og dermed være et nyttig verktøy for å vurdere hva som skal sikres, hvordan det enkelte vannforsyningssystemet skal sikres og hva som kan anses som tilstrekkelig sikring mot den trusselen som er avdekket i analysen. I denne veilederen gjøres likevel et forsøk på å gi en overordnet beskrivelse av en god grunnsikring av de ulike delene av vannforsyningen. Dette gjøres for å gi vannverkene en bedre forståelse for hva som kan anses som en god grunnsikring. Listen er imidlertid ikke uttømmende og skal ikke brukes som en erstatning for en ROS-analyse.

Veilederen oppsummeres avslutningsvis i en overordnet sjekkliste for hvordan vannverkene kan oppnå en tilstrekkelig sikring av sine vannbehandlingsanlegg og distribusjonssystemer. Sjekklisten inneholder administrative og organisatoriske sikringstiltak, så vel som fysiske og elektroniske sikringstiltak. Sjekklisten følger under:

- Alle vannverk bør ha oppdaterte risiko- og sårbarhetsanalyser
- Alle vannverk bør etablere rutiner for bakgrunnssjekk og oppfølging av ansatte
- Alle vannverk bør etablere en god sikkerhetskultur og gode rutiner for sikkerhetsopplæring
- Alle vannverk bør ha etablerte rutiner for informasjonssikkerhet
- Alle vannvannverk bør ha etablert ulike fysiske barrierer og andre forsinkende/avskrekkende tiltak
- Alle vannverk bør kontrollere adgangen til de viktigste delene av vannforsyningen
- Alle vannverk må ha etablert systemer for deteksjon
- Alle vannverk må ha etablert systemer for verifikasjon
- Alle vannverk må ha etablert en reaksjonsplan for å varsle ansatte, politi, abonnenter, myndighetene o.l.
- Alle vannverk må ha planer og rutiner for gjenoppretting og skadereduserende tiltak
- Alle vannverk må ha beredskapsplaner og gjennomføre beredskapsøvelser
- Alle vannverk bør registrere avvik, sikkerhetsbrudd og sikkerhetstruende hendelser
- Alle vannverk må sikre sine data- og driftssystemer (beskrives i egen rapport)

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.norskvann.no

Report no: 229/2017
Report title: Safeguarding and securing water supply facilities against premeditated and malicious acts
Date of issue: 31.12.2017

Author: Leif Riis, Anniken Hareide

ISBN 978-82-414-0403-0 (printed edition)
ISBN 978-82-414-0404-7 (electronic edition)
ISSN 1504-9884 (printed edition)
ISSN 1890-8802 (electronic edition)

Summary

A new regulations regarding drinking water (Drikkevannsforskriften) came into effect January 1st 2017; this pose stricter requirements to water authorities regarding securing water supply facilities. Taking into account todays security threat assessment against Norway, this means the ability to safeguard and secure against premeditated and unwanted attacks, such as acts of terror, espionage, sabotage, vandalism and other criminal acts.

Many of today's water treatment facilities and distribution systems were built decades ago, at a time when the security threat and guidelines for securing and maintaining water supplies was quite different. In many situations therefore, both the water treatment facilities and the distribution systems do not meet the demands of current regulations, nor have the ability to handle potential threats against them.

The purpose of this guide is to provide more information to owner and operators regarding effectively safeguarding and securing water supply facilities against premeditated and malicious acts of terror. These security countermeasures will have the potential to prevent, stop and reduce the consequences of acts of terror. The guide is divided into three main sections; chapter titles are posed as questions that will give the reader an understanding of what subject the chapter intends to focus on. The following is a short summary of the three main sections.

Why do water supplies need securing?

The supply of Norway's drinking water is categorised as critical national infrastructure by The Norwegian Directorate for Civil Protection (Direktoratet for samfunnssikkerhet og beredskap/DSB). Access to fresh water is a fundamental prerequisite for maintaining life and is important with regard to hygiene and sanitation. Failure in the supply of fresh drinking water could also have the potential to disrupt other critical functions such as food production, health care and industry.

The new regulation sets minimum requirements with regard to the quality, quantity and supply of water. Paragraph 10 requires that water treatment plants and distribution system to have sufficient physical security measures. The term sufficient is quite vague, but can be interpreted as a series of security measures that include physical, electronic, administrative and organizational security.

What needs to be secured, and against whom do we secure?
The most fundamental question that needs addressing before planning any security measures is determining what assets you possess, and which assets need to be secured. Water authorities must therefore identify and rank all assets belonging to the water supply system according to the negative consequence to the water system should that asset be removed or destroyed. The ranking of assets is the starting point for determining what assets should be secured and how well they should be secured.

A number of acts relating to terror, espionage, sabotage, vandalism and other criminality could affect Norwegian water fresh water supplies. These acts could range from telephone call bomb threats, vandalism and burglary; they could involve explosives and other forms of physical sabotage, they could also rely on a computer virus that could deactivate security systems or even poison the water using forms of chemical, biological, or radiological substances. It is possible to imagine attacks against pumping stations, water treatment facilities,

water pipelines and direct supply to specific buildings. Attacks on water facilities could be perpetrated as acts of vandalism, acts by mentally unstable people, disgruntled employees or in crises situation sabotage from foreign military powers.

It is important to note that this chapter is not designed to be an official threat assessment of Norwegian water supplies but more of a guide that owner of water treatment plants can use while developing their own threat assessments. The reason for this is that all water supply systems are exposed to different kinds of threats that are dependant on factors such as size and location, as well as who and or what the water is supplying. It is crucial therefore that every water authority make their own threat assessment to determine which threats are relevant to them.

How to secure water supply systems? Principles and best practice

Security countermeasures should be good enough to cause a potential attacker to consider the likelihood of a successful attack as being low. Security countermeasures would therefore act as an effective deterrent. If an attacker nevertheless decides to go through with an attack, measures must be in force to be able to detect the attack as quickly as possible, delay an attacker and to deploy counter measures to reduce potential damage. To achieve this level of security a comprehensive security system should be established that would consist of physical barriers, detection, verification, reaction and recovery. For security measures to have the desired effect it is important that a healthy security culture is established within the organisation. It is people that ultimately implement the organisations technical and organisational security measures. Employees that either do not understand or do not agree with an organisations security culture could quickly reduce the effect of expensive physical and electronic security measures.

In Norway there are several thousand waterworks. These range from small private waterworks that supply small villages, to large public waterworks that supply water to over a hundred thousands households. It is not possible to describe security countermeasures that could be implemented for all of these waterworks. This is due to the enormous variation in design and construction as well as the different water supply systems that can be exposed to different types of threat according to vulnerability, size, location and who the end consumer of water is.

A risk-and vulnerability analysis would help determine what level of basic security and additional security would be appropriate. An analysis would assess an organisations assets, the vulnerability of these assets with regard to a selection of different threat scenarios, assess risk and propose how to manage the risk. This type of analysis would give the water authorities a guide to the risk they face and would be a valuable tool to assess what should be secured, how individual waterworks should be secured and what would be considered an appropriate level of security with regard to a potential threat defined in the analysis. This guide attempts to provide an overall description of good basic security countermeasures for the different parts of a water supply system and to give water authorities a better understanding of what can be considered good basic security countermeasures. This is not a complete list and should not be use as a replacement for a risk-and vulnerability analysis.

The guide is summarised with a checklist for how the owner of waterworks can achieve the appropriate security-level for their water treatment plants and distribution system. The checklist contains administrative, organizational, physical and electronical security countermeasures.

- All waterworks should have risk and vulnerability analysis for their system
- All waterworks should establish routines for background check and system for security follow-up with
- the employees
- All waterworks should establish a good security-culture and routines for security-trading
- All waterworks should have routines for information-security
- All waterworks should have physical and other countermeasures to delay an offender
- All waterworks should secure the most important parts of the supply system in own sections
- All waterworks must have a system for detection of attacks, and the verification of such events
- All waterworks must have a plan to alert employees, local authorities, police and suppliers
- All waterworks must have a plan and routines for recovery and damage decreasing measures
- All waterworks must have a contingency plan and perform contingency exercises
- All waterworks must have a reporting-system in relevance to security
- All waterworks must secure their data and operations (described in other reports)

Innhold

1. Innledning

1.1. Veilederens bakgrunn og formål

Den nye drikkevannsforskriften, som trådte i kraft 1. januar 2017, stiller skjerpede krav til vannverkenes beredskap og forebyggende sikkerhetsarbeid. Med det trusselbildet som Norge står ovenfor i dag innebærer dette også å sikre seg mot tilsiktede uønskede handlinger som terror, etterretningvirksomhet, sabotasje, hærverk og annen kriminalitet. Mange av dagens vannbehandlingsanlegg og distribusjonssystemer ble bygget for flere tiår siden, da både trusselsituasjonen og kravene fra myndigheteneikke var like tydelige som de er i dag. I mange tilfeller vil derfor disse anleggene og systemene hverken tilfredsstille dagens forskriftskrav eller ha mulighet til å håndtere trusler de kan blir utsatt for i dag og i fremtiden. Formålet med denne veilederen er følgelig å gi vannverkene mer kunnskap om effektiv sikring av bygg og anlegg mot tilsiktede uønskede handlinger, slik at de kan gjennomføre sikringstiltak som vil kunne forebygge, forhindre og redusere konsekvensene av slike hendelser.

Kapitlene i denne veilederen som beskriver sikringsteori, sikringsprinsipper og metoder for sikring er i stor grad basert på Forsvarsbyggs Sikringshåndbok. For en mer inngående beskrivelse av disse temaene vises det derfor til Sikringshåndboka.[1)]

Da sikring av vannbehandlingsanlegg og distribusjonssystemer mot tilsiktede uønskede handlinger er et relativt nytt fokusområde vil det være nødvendig at denne veilederen oppdateres og utvikles etter hvert som vannverkene får mer praktisk erfaring med sikring og/eller det kommer en ny lov eller forskrift som stiller andre krav til sikring mot tilsiktede uønskede hendelser.

1) Forsvarsbygg, Sikringshåndboka, 2016

1.2. Mandat og målgruppe

Prosjektbeskrivelsen datert september 2015 lister opp at følgende elementer skal gjennomføres i prosjektet:

1. Innhenting av erfaring gjennom dialog med et utvalg vannverk som har arbeidet med, og gjennomført fysisk sikring av sine anlegg. Hvilke problemer har disse vannverkene støtt på? Hvilke problemstillinger er spesielle for vannverkssektoren?
2. Vurdering av om dagens system for fastsettelse av trusselnivå er funksjonelt. Dialog med sentrale aktører som deltar i fastsettelsen av trusselvurdering og erfaringer fra punkt 1 over (dialog med vannverkene). Forslag til hvordan dagens rutiner for fastsettelse av trusselnivå eventuelt kan forbedres.
3. Veiledning i hvordan vannverkene kan jobbe seg frem (beskrivelse av prosedyre/best practice utfra punktene 1 og 2 over) til fastsettelse av nødvendig sikringsnivå.
4. Systematisering av foreliggende informasjon om fysisk sikring (fra Forsvarsbygg veiledere, andre retningslinjer og normer/standarder). Målsettingen er å forenkles informasjonen (gjerne i tabeller eller tilsvarende) slik at vannverkseier på en enkel måte kan ha forståelse for hvilke krav som skal stilles ved de ulike nivåer av sikring. Og deretter kunne følge opp og kvalitetssikre de sikringstiltakene som gjennomføres.
5. Innhente og gjennomgå erfaringer med håndtering av risikoabonnenter i dialog med utvalgte vannverk, Vannkomiteen i Norsk Vann og Mattilsyn. Utfra dette foreslå rutiner for håndtering av risikoabonnenter.

I løpet av prosjektperioden har prosjektledelsen og styringsgruppen vurdert at punkt 5 ikke naturlig hører hjemme i dette prosjektet. En har imidlertid valgt å ta med konkrete beskrivelser av aktuelle sikringstiltak for ulike deler av vannforsyningsanleggene. Dette er en meny som vannverkseier kan velge fra, etter at det er gjennomført en ROS-analyse og trusselvurdering basert på lokale forhold.

Målgruppen for rapporten er primært vannverkseiere. Veiledningen er aktuell for både små og store kommuner og selskaper. Tilsynsmyndigheter, rådgivere og leverandører forventes imidlertid også å ha nytte av rapporten.

1.3. Veilederens avgrensninger

Vannforsyningen kan rammes av en rekke ulike uønskede hendelser. Denne veiledningen er avgrenset til å omhandle tilsiktede uønskede handlinger (*security*), og tar derfor ikke for seg hendelser som ulykkeshendelser, naturkatastrofer eller teknisk svikt (*safety*). Det er videre foretatt en avgrensning ved at det kun er forhold som omhandler sikring av eiendom, bygg og anlegg som berøres. Dette innebærer at IT-sikkerhet ikke berøres i denne veilederen.[2)]

2) For mer om IT- og annen sikkerhetsstyring se: Norsk vann, *Sikkerhet og sårbarhet i driftskontrollssystemer for VA-anlegg*, Norsk vann-rapport: 195/2013 og Norsk vann, *Sikkerhetsstyring for vannbransjen*, Norsk vann-rapport: 213/2015, 2015

Safety	**Security**
Utilsiktede uønsket hendelse	Tilsiktet eller villet uønsket handling
Ulykkeshendelser, naturkatastrofer eller teknisk svikt	Terror, etterretning, sabotasje, hærverk og annen kriminalitet

Figur 1 *Forskjellen mellom Safety og Security*

1.4. Veilederens oppbygning

Denne veilederen består av tre hoveddeler, delt inn i seks kapitler. Med unntak av innledningskapittelet er alle kapitteloverskriftene formulert som spørsmål for å gi lesere en god forståelse for hva hvert kapittel tar sikte på å svare på.

Den første delen av veilederen består av kapittel 1 og 2, og er en introduksjon av temaet og en beskrivelse av gjeldene lovkrav til sikring av vannforsyningen.

Den andre delen av veilederen består av kapittel 3 og 4. Kapittel 3 gir en innføring i verdivurderinger og belyser hvilke deler av vannforsyningen som kan være relevante å sikre, mens i kapittel 4 diskuteres hvilke trusler den norske vannforsyningen kan stå ovenfor i dag. Kapittelet er ikke ment som en fullverdig trusselvurdering for alle norske vannverk, men som et grunnlagsdokument som vannverkene kan ta i bruk i utarbeidelsen av egne trusselvurderinger.

I den tredje og siste delen av veilederen, kapittel 5 og 6, tar for seg sikring i teori og praksis. Kapittel 5 gir en innføring i grunnleggende sikringsprinsipper, metoder for sikring og sikkerhetshetskultur. I kapittel 6 blir sikringsprisnippene og metodene for sikring satt ut i praksis.

2. Hvorfor må vannforsyningen sikres?

2.1. Samfunnskritisk funksjon

Norges vannforsyning, bestående av drikkevannsforsyning og avløpshåndtering, er utpekt av Direktorat for samfunnssikkerhet og beredskap (DSB) som en kritisk samfunnsfunksjon. En samfunnsfunksjon blir i NOU 2006:6 *Når sikkerheten er viktigst definert som kritisk dersom bortfall av den får konsekvenser som truer befolkningens og samfunnets grunnleggende behov (mat, vann, varme, trygghet og liknende).* Denne veilederen tar kun for seg drikkevannsforsyningen. Drikkevann defineres her ikke bare som drikkevann, men som alt vann som tar ut av en vannkilde for forbruk i boliger, næringsliv eller i samfunnet for øvrig.

I DSB-rapport: *Samfunnets kritiske funksjoner,* utgitt i 2016, vises det til at drikkevannsforsyningen vurderes som kritisk fordi tilgang på vann er en grunnleggende fysiologisk forutsetning for alt liv og er viktig av hygieniske og sanitære årsaker. Svikt i drikkevannsforsyningen vil også kunne få konsekvenser for samfunnets evne til å ivareta en rekke andre kritiske funksjoner. Både matproduksjon, helsevesenet og industri er for eksempel avhengig av tilstrekkelig tilgang på vann. Det vises også til at siden infrastrukturen for vannforsyning er naturlig monopol, er det i utgangspunktet ingen overlappende systemer for innbyggere og næringsliv dersom tjenesten svikter. Dette forsterker behovet for robuste løsninger, god beredskap og redundans på området.

Videre i rapporten beskriver DSB hvilke funksjonsevner samfunnets kritiske funksjoner må opprettholde til enhver tid. For drikkevannsforsyningen beskrives denne funksjonsevnen som «evnen til å levere tilstrekkelig mengde drikkevann til befolkningen og virksomheter med kritisk samfunnsfunksjon». Det vises til at med «tilstrekkelig evne» menes i normal situasjonen at vannforsyningen skal dekke den til enhver tid rådende etterspørselen fra husholdninger og næringsvirksomhet. Vannforsyningen må i tillegg ha beredskap for å sikre forsyningen av et minimumskvantum drikkevann uansett hvilke hendelser som må inntreffe. Dette kvantumet defineres av de ansvarlige myndighetene. Vannforsyningssystemene skal også normalt kunne forsyne brann- og redningstjenestene med slukkevann til brannslukking.

Det er sektordepartementet som har overordnet ansvar for sikkerheten og for å samordne sikkerhetsarbeidet i egen sektor. For vannverkene vil dette være Helse- og omsorgsdepartementet (HOD). Alle virksomheter som har ansvar for kritisk infrastruktur har imidlertid ansvar for å planlegge for å kunne opprettholde sin virksomhet. Som en viktig del av slik kontinuitetsplanlegging inngår det å kartlegge egen sårbarhet og iverksette tiltak for å redusere denne. Det er eierne og operatørene av infrastrukturene som er ansvarlig for sikkerheten og funksjonsdyktigheten i systemene. Myndighetenes rolle i denne sammenheng er å være pådriver, veilede, stille krav og føre tilsyn.

2.2. Krav fra myndighetene

2.2.1. Sikkerhetsloven og drikkevannsforskriften

Det er kun noen få vannverk i Norge som er klassifisert som skjermingsverdige objekter i henhold til lov om forebyggende sikkerhetstjeneste (sikkerhetsloven). Sikkerhetslovens krav til skjermingsverdige objekter vil derfor ikke beskrives nærmere i denne veilederen. Det skal imidlertid nevnes at det per dags dato arbeides med et forslag til ny sikkerhetslov. Det er forventet at kritisk infrastruktur/kritiske samfunnsfunksjoner vil komme til å få en mer sentral rolle i den nye loven.

Den norske vannforsyningen blir i dag regulert blant annet av drikkevannsforskriften. Forskriften stiller krav til vannverkseierne med hensyn til kvalitet, mengde og leveringssikkerhet for drikkevann. Videre pålegger folkehelseloven kommunene ansvar for å sikre at befolkningen faktisk har nødvendig tilgang på trygg og sikker vannforsyning. For denne rapporten fremstår drikkevannsforskriften § 9, 10 og 11 om leveringssikkerhet, forebyggende sikkerhet og beredskap som særlig relevante, da de stiler krav til sikring. De tre paragrafene sier i kort følgende:

§ 9 Leveringssikkerhet – Vannverkseieren skal sikre at vannforsyningssystemet er utstyrt og dimensjonert samt har driftsplaner og beredskapsplaner for å kunne levere tilstrekkelige mengder drikkevann til enhver tid.

§ 10 Forebyggende sikkerhet – Vannverkseieren skal sikre at vannbehandlingsanlegget og alle relevante deler av distribusjonssystemet er tilstrekkelig

fysisk sikret, og at alle styringssystemer er tilstrekkelig sikret mot uautorisert tilgang og bruk.

§ 11 Beredskap – Vannverkseieren skal sikre at det gjennomføres nødvendige beredskapsforberedelser og utarbeides beredskapsplaner i samsvar med helseberedskapsloven og forskrift om krav til beredskapsplanlegging.

I § 9 stiller drikkevannsforskriften krav om at vannforsyningen skal sikres for å kunne levere tilstrekkelig drikkevann til enhver tid. Også i krise eller katastrofe i fredstid eller ved krig skal vannforsyningen opprettholdes for å sikre vann til nødvendige formål. Sikring av vannforsyningen i krise/krig vil imidlertid ikke behandles i denne veilederen. Grunnsikringen som blir anbefalt vil imidlertid også kunne ha en viss effekt ved en slik situasjon, men i tillegg vil man være avhengig av vakthold og sikring fra militære styrker.

Forskriftens § 10 stiller altså krav om at vannbehandlingsanlegget og alle relevante deler av distribusjonssystemet skal være tilstrekkelig fysisk sikret. Hva som menes med «tilstrekkelig fysisk sikring» utdypes imidlertid ikke. Innen sikringsfaget blir begrepet fysisk sikring gjerne brukt som en samlebetegnelse for fysiske sikringskomponenter som gjerder, porter, vegger, vinduer og dører. Fysisk sikring utgjør en helt sentral del av sikringen, men for å etablere en god sikring inngår også elektronisk sikring, så vel som menneskelige og organisatoriske sikringstiltak. Sammen utgjør disse det som blir kalt en *helhetlig sikring*.
I lys av drikkevannsforskriftens formålsbestemmelse i § 1 tolkes *tilstrekkelig fysisk sikring* i denne veilederen som *tilstrekkelig helhetlig sikring*, bestående av fysisk og elektronisk sikring samt administrative og organisatoriske sikringstiltak (menneskelige sikringstiltak). For mer om helhelhetlig sikring se delkapittel *5.1.3 Helhetlig tilnærming til sikring* (se kap. 5.3).

I *Veileder til drikkevannsforskriften*, utgitt av Mattilsynet i august 2017, vises det til at hvilke deler av vannforsyningssystemet som er relevante å sikre og hva som anses som *tilstrekkelig* må vurderes for hvert enkelt vannforsyningssystem.[3)] Mattilsynet viser til at rapporter og veiledere utgitt av bransjeforeninger som Norsk Vann eller offentlig etater som DSB og Folkehelseinstituttet vil kunne hjelpe vannverkseierne med å vurdere disse spørsmålene. Denne veilederen har som formål å hjelpe vannverkene med slike vurderinger.

3) Mattilsynet, Veiledning til drikkevannsforskriften, 2017, 17-19

Figur 2 *Illustrasjon av en helhetlig sikringtilnærming. Illustrasjonen viser overordnede sikringstiltaksgrupper som inngår i en helhetlig sikring. De ulike sikringstiltakene har som formål å til sammen forebygge, avskrekke, forsinke, detektere, verifisere, varsle, stoppe/ta kontroll og bidra til å gjenopprette normaltilstanden etter en uønsket hendelse. For at sikringstiltakene skal fungere etter hensikt må organisasjonen også ha en god sikkerhetskultur.*

I § 11 stilles krav om at vannverkene skal ha en beredskapsplan som gjør dem i stand til å håndtere uønskede hendelser. I Mattilsynets veiledning stilles krav om at det skal ligge en helhetlig risiko- og sårbarhetsanalyse (ROS) til grunn for arbeidet med å etablere beredskapsplanverk. En god ROS-analyse skal avdekke alle utfordringer som kan oppstå både ved ordinær drift, og under kriser eller katastrofer eller ved krig. De ordinære driftsfarene skal forebygges, fjernes eller reduseres til et akseptabelt nivå gjennom farekartleggingen og farehåndteringen. ROS-analysen og beredskapsplanene skal evalueres ved jevne mellomrom og/eller dersom noen av innsatsfaktorene i ROS-analysen (verdi, trussel, sårbarhet) endrer seg. Videre er det avgjørende at det gjennomføres beredskapsøvelser.[4)] Norsk Vann har utarbeidet en rekke rapporter, aksjonsplaner og veiledere for sikkerhet og beredskap som gir råd om hvordan vannverkene skal etablere en god beredskap og beredskapsplanverk for drikkevannsforsyningen.[5)]

4) Mattilsynet, *Veiledning til drikkevannsforskriften*, 2017, 17-19

5) For en fullstendig oversikt over rapporter fra Norsk Vann se: https://norskvann.no/index.php/vann/sikkerhet-og-beredskap. Se spesielt: Norsk Vann, Sikkerhetsstyring for vannbransjen, Norsk Vann-rapport: 213/2015 og Mattilsynet, Økt sikkerhet og beredskap i vannforsyningen – fra ROS til operativ beredskap (veiledning), 2017

Figur 3 *Relevante Norsk Vann rapporter*

2.3. Omdømme og forventninger

Et godt omdømme er svært viktig for drikkevannsforsyningen. Både befolkningen og industrien må være trygg på at vannet som leveres ikke er helsefarlig og at man kan regne med en stabil og kontinuerlig leveranse.

Dårlig sikkerhet vil utvilsomt kunne ha en negativ effekt på vannforsyningens omdømme. De siste årene har det vært en rekke saker i media som omtaler sikringen av norske vannforsyningssystemer negativt.[6)] Det kan forventes at en slik negativ omtale vil eskalere dersom en uønsket tilsiktet hendelse faktisk skulle inntreffe. Hvor stor den negative effekten på omdømme vil være avhenger imidlertid av hendelsens konsekvenser, og i hvilken grad vannverkene har lykkes med å begrense skadeomfanget med å implementere sikringstiltak.

Et forhold som trolig vil ha stor påvirkning på vannforsyningens omdømme vil være kommunikasjon ut til befolkningen. Det er avgjørende at informasjonen kommer raskt ut og at den er korrekt. Mangelfull eller feilaktig informasjon vil kunne skape stor usikkerhet og derfor gjøre betydelig skade på omdømme.

En sikkerhetstruende hendelse kommer som regel svært overraskende. En slik hendelse vil kreve at man raskt lokaliserer skaden, vurderer og reduserer skadeomfanget. Spesielt hendelser som skaper frykt i samfunnet, som for eksempel et terrorangrep, har potensiale til å alvorlig kunne skade omdømme. Dette skyldes blant annet at en slik hendelse vil få stor medieoppmerksomhet. Dersom det kommer frem at en slik hendelse skyldes dårlig sikkerhetskultur eller mangelfulle sikringstiltak, som i tillegg ikke tilfredsstiller myndighetenes krav, vil dette kunne få alvorlige konsekvenser for omdømme. Dette vil igjen kunne resultere i erstatningskrav eller at ledelse/styret kan bli tvunget til å trekke seg fra sine stillinger.

6) Kirkebøen, Stein Erik, «Hemmelig rapport fra 2013 med kraftig kritikk av Oslos drikkevannssikring, 17.06.2015, https://www.aftenposten.no/osloby/i/q8no/Hemmelig-rapport-fra-2013-med-kraftig-kritikk-av-Oslos-drikkevanns-sikring, Kirkebøen, Stein Erik, Aslabeehg: - Byrådet har ikke gjort nok med vannsikkerheten, 17.06.17, https://www.aftenposten.no/osloby/i/O1nV/Alsabeehg---Byradet-har-ikke-gjort-nok-med-vannsikkerheten og Johnsrud, Ingar m.fl., «Kunne ha stippet vanntilførselen med mobilen», 09.09.11, https://www.vg.no/nyheter/innenriks/terrortrusselen-mot-norge/kunne-stoppet-vanntilfoerselen-med-mobilen/a/10098352/

3. Hva er viktig å sikre?

3.1. Verdi- og skadevurdering

Et av de mest grunnleggende spørsmålene som skal stilles når man setter i gang med sikrings- og sikkerhetsarbeid er hvilke verdier virksomheten har, og hva som skal sikres. Begrepet verdi kan defineres som en «ressurs som hvis blir utsatt for uønsket påvirkning, vil medføre en negativ konsekvens for den som eier, forvalter eller drar fordel av ressursen».[7)] En verdi kan være funksjoner, fysiske objekter, nøkkelpersonell eller informasjon som en virksomhet er avhengig av for å utføre sine kjerneoppgaver.

Før vannverkene går i gang med å sikringsarbeidet må det altså gjennomføres en verdivurdering av det aktuelle vannforsyningssystemet og alle relevante elementer knyttet til dette.. En verdivurdering er en kartlegging og rangering av en virksomhets verdier. Det vil si en prosess for identifisering og rangering av verdier og vurdering av konsekvenser dersom verdiene fjernes, skades eller ødelegges.

3.1.1. Identifisering av verdier

Enhver virksomhet må identifisere og vurdere hvilke leveranser og prosesser som er sentrale for egen drift, og hvilke verdier som understøtter disse leveransene. For vannverkene vil hovedleveransen være å levere tilstrekkelig mengde rent vann til befolkningen og virksomheter med kritiske samfunnsfunksjoner. Verdien som understøtter hovedleveransen vil for eksempel være ansatte med spesialkompetanse og/eller bygg, anlegg og infrastruktur som er spesialtilpasset for vannforsyning. Vannverkene bør også vurdere hvordan og i hvilke grad de er avhengig av andre virksomheter, for eksempel virksomheter som leverer strøm eller teletjenester.

3.1.2. Rangering av verdier og skadevurdering

Generelt henger verdiens betydning sammen med de konsekvenser det vil ha for virksomheten dersom den faller bort. NSMs *Veileder i verdivurdering* påpeker at når verdiene er definert, bør de rangeres etter viktighet, for eksempel ved at de foreles på nivåene LAV, MODERAT, HØY og SVÆRT HØY som tar utgangspunkt i ulike kriterier.[8)]

Verdi	Konsekvens
Lav	Tap eller reduksjon av verdi har små konsekvenser
Moderat	Tap eller reduksjon av verdi kan ha store konsekvenser
Høy	Tap eller reduksjon av verdi har store konsekvenser
Svært høy	Tap eller reduksjon av verdi har umiddelbare og svært alvorlige konsekvenser

Figur 4 *Eksempel på rangering av verdier*

Verdivurderingen henger altså i praksis tett sammen med skadevurderingen. Å gjennomføre en skadevurdering innebærer å vurdere konsekvenser ved bortfall eller ødeleggelse av en verdi, og foreta en vurdering av skadepotensialet dersom en verdi blir utsatt for en sikkerhetstruende hendelse. Normalt er derfor skadevurderingen et hjelpemiddel eller en utdypning av konsekvensvurderingene i verdivurderingen. Vannverkene kan ta utgangspunkt i følgende hovedkategorier i vurdering av konsekvens ved verdienes bortfall:

Liv og helse
Bortfall av drikkevannsforsyningen vil kunne få store konsekvenser som befolkningens liv og helse. Dette som følge av at tilgang på vann er en grunnleggende fysiologisk forutsetning for alt liv og viktig av hygieniske og sanitære årsaker.

Daglig drift og operativ evne
Svikt i drikkevannsforsyningen vil kunne få konsekvenser for samfunnets evne til å ivareta en rekke andre kritiske funksjoner. Både matproduksjon, helsevesenet og industri er for eksempel avhengig av tilstrekkelig tilgang på vann.

Informasjon
Tap eller kompromittering av sensitiv informasjon vil være uheldig da dette kan brukes av en trusselaktør til å planlegge et anslag.

Økonomi
Økonomiske kostnader knyttet til erstatning av ødelagt utstyr, skade på bygninger eller nedetid/forsinkelser ved viktige leveranser for eksempel til industrien.

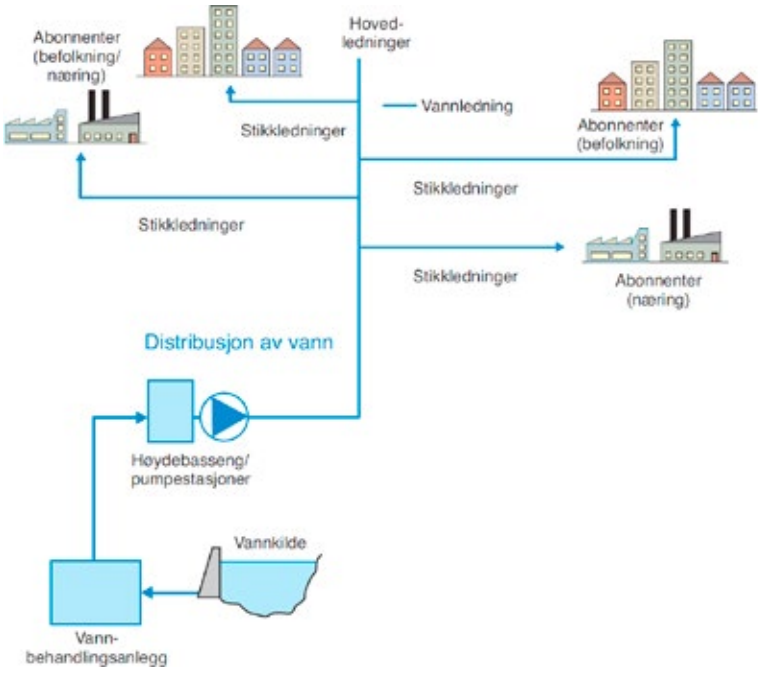
7) Norsk standard 5830:2012 *Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Terminologi*

8) NSM, *Veiledning i verdivurdering*, 2009

Omdømme
Svekket omdømme eller redusert tillit i befolkningen kan komme som følge av en uønsket hendelse. Denne kategoriene er ofte nært knyttet til de fire overstående områdene og kommer gjerne som en konsekvens av dem.

3.2. Vannforsyningens sentrale deler

I dette delkapittelet følger en kort gjennomgang av de meste sentrale delene av vannforsyningsprosessen fra vannkilden til abonnentene. Vannforsyningsprosessen illustreres i figuren under.



Figur 5 *Illustrasjon av vannforsyningens sentrale deler*

Vannkilde og råvannsinntak
I Norge skiller man grovt sett mellom to typer vannkilder: overflatevannkilder og grunnvannskilder. Innsjøer, tjern, elver og bekker er eksempler på overflatevannskilder. 90 % av drikkevannet kommer fra slike kilder. De resterende 10 % kommer fra grunnvannskilder som rørbrønner i løsmasser, borebrønner i fjell og andre løsninger.

Vann hentes fra vannkilden via et råvannsinntak, som består av blant annet inntaksledninger, pumper og ventiler. Mens inntaksledningen gjerne befinner seg på bunnen av vannkilden, er pumpene og ventilene plassert i et bygg eller annen installasjon i nærhet av kilden. Disse pumpene og ventilene er tilkoblet et driftsstyringssystem som overvåker og regulerer vanninntaket. Byggene/installasjonene er gjerne ubemannet.

Vannbehandlingsanlegg
Vannbehandling er en vesentlig del av vannforsyningen i Norge og finner sted i vannbehandlingsanleggene. Hovedformålet med behandlingen av drikkevann er å inaktivere mikroorganismer (desinfeksjon), fjerne partikler og organisk materiale (humus), fjerne andre uønskede uorganiske stoffer og tilpasse vannkvaliteten til ledningsnettet (korrosjonskontroll). I Norge er det krav til at vannbehandlingen og kildebeskyttelsen til sammen skal gi tilstrekkelige hygieniske barrierer.[9)]

For større vannverk er gjerne andre funksjoner plassert i eller i nærheten av vannbehandlingsanlegget. Det kan f. eks være administrativ og teknisk ledelse, driftsentral, dataservere, kommunikasjonssystem. Større vannverk vil i mange tilfeller også ha en døgnbemannet driftssentral på eller ved vannbehandlingsanlegget.

Distribusjons av vann via ledningsnettet
I Norge består ledningsnettet av 41 000 km med vannledninger. I tillegg til dette kommer stikkledningsnettet til og fra bygninger.

Ledningsnettet består av et transportsystem for vann bestående av pumpestasjoner og høydebasseng.[10)] Pumpestasjonene er mindre bygg/installasjoner med pumper for å skape/opprettholde trykk i ledningsnettet, eller leder vann over en høyde i terrenget. Høydebassenger er vannmagasiner som bygget for å utjevne belastningen på vannforsyningssystemet, samt utjevne trykket og sikre tilgang på vann ved kortvarig driftsstans og utjevne trykket.

9) Drikkevannsforskriften § 13 Vannbehandling.Tilgjengelig på: https://lovdata.no/dokument/SF/forskrift/2016-12-22-1868

10) Norsk vann, «Ledningsnettet», 26.06.13. Tilgjengelig på: https://norskvann.no/index.php/vann/ledningsnett

4. Hvem og hva skal vi sikre oss mot?

Begrepet trussel brukes om både *kapasitet og intensjon* til gjennomføre uønskede handlinger. I norsk straffelov brukes trusselbegrepet om aggressive ord eller handlinger. I denne veiledningen defineres trussel som «en mulig uønsket handling som gir en negativ konsekvens for en entitets sikkerhet».[11] For å systematisere trusselbildet blir truslene delt inn i følgende trusselkategorier: terror, sabotasje og annen kriminalitet (tyveri, hærverk). I tillegg blir etterretning inkludert som en egen kategori. Etterretning må imidlertid her betraktes som et første ledd i forberedelsesfasen til gjennomføring av kriminelle handlinger, sabotasje- eller terroraksjoner.

I dette kapittelet følger en gjennomgang av trusler som per desember 2017 vurderes som aktuelle for vannforsyningen i Norge. Denne gjennomgangen må ikke forstås som en offisiell trusselvurdering, men som et grunnlagsnotat som vannverkene kan benytte i utarbeidelsen av egne trusselvurderinger. Dette følger blant annet av at det trusselbildet som de ulike vannverkene står ovenfor vil endre seg etter forhold som for eksempel størrelse, beliggenhet, og ikke minst hvem eller hva det aktuelle vannverket forsyner. Det er derfor avgjørende at hvert enkelt vannverk foretar en egen trusselvurdering for å kartlegge relevante trusler. Kilder for trusselvurderinger kan være både åpne og graderte kilder, for eksempel fra Politiets sikkerhetstjeneste (PST), Nasjonal sikkerhetsmyndighet (NSM) og Etterretningstjenesten (E-tjenesten). Det kan også være relevant å benytte seg av statistikk, rapporter og forskningsartikler. For utvalgte vannverk kan det være aktuelt å få bistand fra politiet eller andre med fagkompetanse på området for å utarbeide en slik trusselvurdering.

11) Standard Norge, «Norsk standard 5830: 2012 Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Terminologi», (Oslo: Standard Norge, 2012)

4.1. Trusselbilde og trusselaktør

4.1.1. Terror

Ifølge PST og E-tjenesten er den mest alvorlige terrortrusselen mot Norge og norske interesser i 2017 knyttet til Den islamske stat i Irak og Levanten (ISIL) og al-Qaida (AQ).[12] Per november 2017 vurderer PST det som mulig[13] at det kan bli gjennomført et terrorangrep i Norge i nærmeste fremtid. Dette begrunnes ved at Norge er en del av fiendebildet til internasjonale terrorgrupper og at det i Norge finnes ekstreme islamister som kan følge oppfordringene til internasjonale terrorgrupper om å begå voldshandlinger der man befinner seg. Vi må derfor være forberedt på at terrorhandlinger kan skje i Norge. Det vises imidlertid til at en eventuell terroraksjon i Norge sannsynligvis vil være av samme type som man har sett ellers i Europa det siste året. Dette betyr metoder som bruk av kniv og kjøretøy mot mål med få sikringstiltak og hvor man kan ramme mange sivile.[14]

Det finnes i dag få oppdaterte kilder som eksplisitt beskriver og vurderer terrortrussel mot norske vannforsyningsanlegg. I FFI-rapporten *Terror mot drikkvann*, som ble utarbeidet av terrorforsker Brynjar Lia og Petter Nesser i forbindelse med DSB-prosjektet *Sårbarhet i vannforsyningen* i 2003. Her vurderes terrortrusselen mot den norske vannforsyningen som lav. Dette begrunnes blant annet med at man historisk har sett svært få terroranslag mot vannforsyningen. De få «vellykkede» terroranslagene man har sett begrenser seg i hovedsak til sabotasje utført med sprengstoff, mens forgiftningsaksjoner har vært ekstremt sjeldne.[15] En gjennomgang FFI gjorde av datamateriale om terrorhendelser viser også at terrorisme mot vannforsyning forekommer svært sjelden sammenlignet med

12) Politiets sikkerhetstjeneste (PST), Trusselvurdering *2017*, PST, 1.02.2017, tilgjengelig på: http://www.pst.no/media/utgivelser/trusselvurdering-2017/

13) Begrepet «mulig» beskrives at politiet, PST og Forsvaret som at «det er like sannsynlig som usannsynlig».
For full oversikt over PSTs bruk av sannsynlighetsord se: PST, *Trusselvurdering 2017*, PST,

14) PST, Vurdering av trusselbildet – november 2017, 22.11.17, tilgjengelig på: https://www.pst.no/alle-artikler/pressemeldinger/vurdering-av-trusselbildet-i-norge---november-2017/

15) Lia, Brynjar og Petter Nesser, «Terror mot drikkevann – En oversikt over terrorgruppers interesse for å ramme offentlig drikkeforsyning», FFI-rapport: 2003/01919 og Bartnes, Jørgen m.fl., *Sårbarhet i vannforsyningen*, 22

terrorisme mot andre typer mål.[16] I forbindelse med utarbeidelsen av denne veilederen har det ikke kommet frem nye opplysninger som tilsier at terrortrusselen mot vannforsyningen bør vurderes høyere enn den ble gjort i 2003. Det skal imidlertid bemerkes at eventuelle graderte kilder om terrortrusler mot vannforsyningen ikke har vært tilgjengelig for gruppen som har arbeidet med veilederen.

Vannforsyningen utgjør en kritisk samfunnsfunksjon som skal ivareta ett av befolkningens grunnleggende behov. Ved svikt eller tap av denne tjenesten, vil konsekvensene være store.[17] Til tross for at terrortrusselen vurderes som lav kan det derfor ikke utelukkes at vannforsyningen i fremtiden kan være et aktuelt terrormål.

Offentlig drikkevann kan rammes av terror på en rekke ulike måter. Anslagene kan strekke seg fra angrep som inkluderer bomber, sprengstoff og andre former for fysisk sabotasje, via dataangrep som lammer sikringssystemene for vannforsyningen til ulike former for forgiftning med kjemiske, biologiske eller radiologiske substanser. Det er mulig å tenke seg anslag mot det sentrale drikkevannreservoaret, pumpestasjoner, renseanlegg, hovedledningsnettet eller tilførselen til spesifikke bygninger med særskilte funksjoner.[18]

Av de få tilfeller der det har forekommet terrorangrep mot den offentlige vannforsyningen har det som oftest vært brukt andre fremgangsmåter enn forgiftning. Den lave forekomsten av generelle forgiftning har bidratt til at denne typen angrep ofte blir avskrevet som urealistiske. Dette følger også av den store mengden giftstoff som er nødvendig for å oppnå dødelig dose. Det er også sjeldent at terrorgrupper har tilgang på og kompetanse til å håndtere de mest potente virkemidlene (toksiner og biologiske våpen).[19]

FFI advarer imidlertid mot å avskrive forgiftningsangrep helt. Det følger av at mengdene giftstoffer som skal til for å oppnå dødelig eller skadelig dose vil avhengig av hvilke stoffer som benyttes, hvor gode rense- og kontrollmekanismene er og størrelsen på det kontaminerte vannreservoaret. Det påpekes at jo mer lokalt rettet et terrorangrep er, desto større er sjansen for at drikkevannet blir forgiftet. Dette begrunnes ved at terrorangrep mot et lite, lokalt vannreservoar eller et mindre lukket vannforsyningsnett har større sjanser for å lykkes enn et anslag mot et større og bedre sikret vannreservoar.[20] Det er således viktig å sørge for at mindre vannverk som forsyner en samfunnsviktig installasjon eller virksomhet også gis en tilstrekkelig sikring.

4.1.2. Sabotasje

Sabotasje utført av fremmede makters spesialstyrker, som anses å ha svært god kunnskap og erfaring på området, vurderes å være en aktuell trussel først ved et relativt høyt konfliktnivå av utenrikspolitisk art. Sabotasje av denne typen anses altså som svært uvanlig i fredstid, og vil normalt bli gjennomført i forkant av krise/krigssituasjon.[21] I en alvorlig krise-/krigssituasjon er det imidlertid forventet at det vil forekomme angrep mot norske verdier. Formålet med et sabotasjeangrep mot den norske vannforsyningen kan være å kutte eller hindre fiendens eller en befolknings tilgang på vann, eller å forårsake oversvømmelse og ødeleggelse.[22] Ved en spent situasjon må det også forventes at fienden vil kunne bruke sabotasje som et virkemiddel for å skape kaos og øve press. Formålet med denne typen aksjoner er ikke nødvendigvis å ødelegge vannforsyningen i seg selv, men for å skremme og tvinge gjennom løsninger på fiendens premisser.[23] En slik modus blir gjerne omtalt som en form for «hybrid krigføring». Kritisk infrastruktur og samfunnskritiske system, som krafts- og vannforsyning samt infrastruktur for kommunikasjon, vurderes som særlig aktuelle mål for denne typen aksjoner.[24]

16) Lia, Brynjar og Petter Nesser, «Terror mot drikkevann – En oversikt over terrorgruppers interesse for å ramme offentlig drikkeforsyning», FFI-rapport: 2003/01919 og Bartnes, Jørgen m.fl., *Sårbarhet i vannforsyningen*, 22

17) DSB, *Samfunnskritiske funksjoner – Hvilke funksjonsevne må samfunnet opprettholde over enhver tid?*

18) Lia og Nesser, «Terror mot drikkevann», 16-17

19) Lia og Nesser, «Terror mot drikkevann», 17 og Claudia Copeland, «Terrorisme and Security Issues Faceing the Water Infrastructure Sector» i Congressional Research Service, 2010, 2

20) Lia og Nesser, «Terror mot drikkevann», 17

21) Forsvarsbygg, *Sikringshåndboka*, 2016, 69

22) Lia og Nesser, «Terror mot drikkevann», 29

23) Etterretningstjenesten, *Fokus 2017 – Etteretningstenesta si vurdering av aktuelle tryggingsutfordringar*, 2017, 34-35

24) Reichborn-Kjennerud, Erik og Patrick Cullen, «What is Hybrid Warefare» i *Policy Breif 1/2016*, NUPI, 2016. og Etterretningstjenesten, *Fokus 2017,* 34-35

Som det også ble vist til i delkapittelet om terror kan et sabotasjeanslag ramme vannforsyningen på en rekke ulike måter. Anslagene kan strekke seg fra angrep som inkluderer bomber, sprengstoff og andre former for fysisk sabotasje, via dataangrep som lammer sikringssystemene for vannforsyningen til ulike former for forgiftning med kjemiske, biologiske eller radiologiske substanser.[25)] Fysiske sabotasjeangrep kan rette seg mot drikkevannreservoaret, pumpestasjoner, renseanlegg, hovedledningsnettet eller tilførselen til spesifikke bygninger med særskilte funksjoner. Sabotasjeaksjoner kan også forberedes og gjennomføres slik at de ser ut som vanlig ulykker forårsaket av menneskelige feil, slurv og manglende kunnskaper, eller fordekt som ulykker.

I E-tjenestens årlige vurdering av den norske sikkerhetssituasjonen, *Fokus 2017*, vises det til at Russland vil fortsette å videreutvikle og teste ut metoder for sabotasje, blant annet mot kritisk infrastruktur. Dette gjøres for eksempel i Ukraina hvor en rekke digitale angrep har vært rettet mot den ukrainske kraftforsyningen.[26)] I norske medier har det blitt reist mistanke om at også Norge kan ha vært utsatt for mindre russiske sabotasjeøvelser. Samtidig som en større russisk militærøvelse ble avholdt øst for den norske grensen i september 2017 mistet norske fly på flyplassen i Øst-Finnmark GPS-signalene. Som følge av at signalene var stabilt borte over tid mistenkes at de var utsatt for jamming[27)]. Det var på forhånd forventet at russerne ville øve på elektronisk krigføring under øvelsen. Forsvaret kan imidlertid ikke bekreftet at russisk jamming var årsaken til at GPS-signalet falt ut, men NSM har gjort gjentatte målinger i Kirkenes-området som viser at forstyrrelsene kom fra øst.[28)]
I internasjonale medier har det blitt spekulert i om Russland har vært innblandet i sabotasje av svenske kommunikasjonmaster som blir brukt til nødkommuni kasjon og for å manipulere navigasjonsutstyr på skip i Svartehavet.[29)]

For vannverkene kan det imidlertid være relevant å vurdere sabotasje ikke bare som en del av opptakten til krise/krig, men også som en handling utført som en reaksjon mot staten, kommunen eller et av vannverkene. At det norske vannforsyningsnettet kan bli utsatt for denne typen handlinger har man blant annet sett eksempel på i Bærum kommune. I september 2017 gikk politiet ut og ba publikum om tips om en person som gjentatte ganger over en periode over åtte år har sabotert vannforsyningen på Snarøya. Personen har flere ganger brutt seg inn i vannkummer på Snarøya og skrudd opp ventiler. Politiet mener mannen er erfaren og har god kjennskap til vannsystemer. Det er ikke kjent for politiet hvilket motiv vedkommende har til å utføre disse sabotasjeaksjonene, men en hypotese går ut på at personen har et dårlig forhold til Bærum kommune og vil ødelegge for kommunen.[30)] Et annet eksempel er fra 1972, da en fortvilet bonde fra Smøla truet med å tømme seks dunker av plantegift i Oslos største drikkevannskilde, Maridalsvannet. Bakgrunnen for aksjonen var at bonden mente staten hadde tatt livsgrunnlaget på nyrydningsgården fra han ved blant annet å innføre moms. Bonden krevde derfor en erstatning på 540 000 kr. Etter en større politiaksjon ble imidlertid mannen overmannet.[31)]

25) Lia og Nesser, «Terror mot drikkevann», 16-17

26) Etterretningstjenesten, *Fokus 2017,* 34-35

27) Jamming er forstyrrelser, blokkering eller fastlåsing av signaler. Teknisk foregår jamming med en støysender

28) Horn, Knut-Sverre, «Støy fra Russland slo ut GPS-signaler for norske fly» på *NRK.no*, 05.10.2017. Tilgjengelig på: https://www.nrk.no/finnmark/stoy-fra-russland-slo-ut-gps-signaler-for-norske-fly-1.13720305

29) Finsveen, Jesper Nordahl, «Tror fremmede makter kan stå bak maktsabotasje i Sverige. Kan være en stresstest ifølge politiet» i Dagbladet, 17.05.16. Tilgjengelig på: https://www.dagbladet.no/nyheter/tror-fremmede-makter-star-bak-mastsabotasje-i-sverige-kan-vaere-en-stresstest-ifolge-politiet/60382242 og Brombach, Harald, «Falske GPS-signaler narret navigasjonsutstyret til flere titalls skip» i Teknisk ukeblad, 11.08.17. Tilgjengelig på: https://www.nrk.no/finnmark/stoy-fra-russland-slo-ut-gps-signaler-for-norske-fly-1.13720305

30) Larsen, Heidi Elisabeth, «Politiet ber om tips: Politiet tror denne vannsabotøren har terrorisert kommunen i åtte år. Nå ber de om hjelp for å stoppe «vannmannen» i Dagbladet, 11.09.2017. Tilgjengelig på: https://www.dagbladet.no/nyheter/politiet-tror-denne-vannsabotoren-har-terrorisert-kommunen-i-atte-ar-naber-de-om-hjelp-for-a-stoppe-vannmannen/68683035

31) Kirkebøen, Stein Erik, «1972: Bonde helt gift i Oslos drikkevann» i *Aftenposten, 16.07.2015. Tilgjengelig på: https://www.aftenposten.no/osloby/i/5vVX/1972-Bonde-helte-gift-i-Oslos-drikkevann*, 16.07.2015. Tilgjengelig på: https://www.aftenposten.no/osloby/i/5vVX/1972-Bonde-helte-gift-i-Oslos-drikkevann

4.1.3. Etterretning

Etterretning betraktes i denne veilederen som et ledd av forberedelsesfasen til gjennomføring av kriminelle handlinger, sabotasje eller terroraksjoner. Etterretning er informasjon og kunnskap tilegnet gjennom observasjon, innsamling, analyse, evaluering. Det antas at en trusselaktør vil kunne utføre en viss form for rekognosering, kartlegging i forkant av et angrep.

Etterretningsaktører blir tradisjonelt sett delt inn i to kategorier: ikke-statlige og statlige aktører. De vil kunne benytte seg av de samme metodene, men intensjonen deres vil være forskjellig. De statlige aktørene vil naturlig være interessert i informasjonen som kan fremme sine nasjonale interesser, mens de ikke-statlige aktørene kan være ute etter informasjon som kan gi fordeler for en bedrift eller kan gjøre gjennomføring av en kriminell handling enklere. I PSTs åpne trusselvurdering for 2017 vises det til at Norge og norske interesser vil utsettes for fremmed etterretningsvirksomhet som kan ha stort skadepotensial. PST trekke frem tre hovedområder som særlig attraktive for utenlandsk etterretning. Disse områdene er forsvars- og beredskapssektoren, politiske beslutningsprosesser og kritisk infrastruktur. Etterretningsvirksomhet mot kritisk infrastruktur har som formål å hente ut informasjon om selve infrastrukturen, samt legge til rette for å kunne manipulere data eller forbedrede sabotasje.[32)] At etterretningstrykket mot kritisk infrastruktur i Norge er høyt ble igjen bekreftet av E-tjenesten og PST på Sårbarhetskonferansen i september 2017. På konferansen uttalte PST-sjef Benedicte Bjørnland til VG at «vi ser store aktører som kartlegger kritisk infrastruktur. Nå er det fredstid, men vi tenker at å kartlegge handler om å skaffe informasjon som kan brukes når situasjonen er mer tilspisset.»[33)]

Uavhengig av hvem som gjennomfører etterretningsvirksomhet og hvorfor, er det noen kjennetegn og metoder som går igjen:

- Kartlegging av åpne kilder som kart, tegninger, rapporter etc. som er offentlig tilgjengelig
- Fotografering av områder, bygninger, sikkerhetsrutiner som er knyttet til objektet m.m.
- Sosial manipulering
  - Infiltrering av ansatte
  - Utpressing av ansatte
  - Hacking (fysisk eller via datanettverket)
  - Avlytting og avlesning på avstand
  - Innbrudd og tyveri for å tilegne seg informasjon

32) PST, *Trusselvurdering 2017*,

33) DSB, *Veileder til helhetlig risiko- og sårbarhetsanalyse i kommunen*, 2014, 14

4.1.4. Annen Kriminalitet (Innbrudd, tyveri og hærverk)

Kriminalitet er handlinger som er straffbare i henhold til straffeloven, og utviklingen innen kriminalitet følger samfunnsutviklingen som sådan.[34)] Kriminelle handlinger motiveres som regel av egen vinning. Hovedforskjellen mellom ulike kriminelle aktører er hvilken kapasitet de har til å gjennomføre handlingen. Mer erfarne aktører vil gjerne benytte seg av mer avanserte metoder sammenlignet med mindre erfarne aktører. Det vil også være ulike verdier de er interessert i.

Alle norske vannverk har verdier som kan være av interesse for kriminelle. Dette kan være lett omsettelig verdier som for eksempel mobiltelefoner, PCer, videokanoner, flatskjermer, sambandsutstyr, verktøy og verdifulle metaller som kobber. Dette er hovedsakelig verdier som man finner i administrasjonsbygninger, men dette kan også finnes i andre bygg/anlegg/installasjoner tilknyttet til vannforsyningssystemet.

Det antas at en kriminell vil kunne utføre en viss form for rekognosering og kartlegging før en anslaget gjennomføres. Trusselaktøren kan også ha fått informasjon fra en utro tjener i organisasjonen eller fra en leverandør. Dersom sikringen av bygget fremstår som god vil imidlertid en vinningskriminell trolig velge et annet og enklere mål.

Fordi bygg/anlegg/installasjoner tilknyttet det norske vannforsyningssystemet ligger lett tilgjengelig og gjerne er plassert på områder med lite eller ingen boligbebyggelse vil de kunne være svært utsatt for hærverk og innbrudd. Dårlig sikkerhetspreg med en svak fysisk sikring, manglende overvåkning og alarmsystemer på bygg som pumpehus, høydebasseng og liknende kan bidra til å forsterke denne trusselen. Man er i dag kjent med en rekke tilfeller der slike bygg har vært utsatt for hærverk som tagging, dører har blitt brutt opp og vinduer som har blitt knust. Det er også registert at personer har tatt seg opp på taket av høydebasseng og dyttet ulike gjenstander inn i vannkammeret gjennom luftekanaler eller inspeksjonsluker som har blitt brutt opp. Funn i forbindelse med rengjøring av bassenger tyder på at det har det gått relativt langt tid før slike hendelser har blitt oppdaget.

Det finnes i dag ingen statistikk over innbrudd, tyveri eller hærverk i bygg/anlegg/installasjoner tilknyttet vannforsyningssystemet, men dette er noe som bør vurderes å etablere på sikt.

34) Kripos, *Trendrapport 2016 – Organisert og annen alvorlig kriminalitet i Norge*, 2016

4.2. Trusselscenarioer

Basert på trusselvurderingen som utarbeides for hvert enkelt vannverk bør det også utarbeides et sett med trusselscenarier[35] som eksempler på ulike uønskede hendelser som kan skje. Disse trusselscenariene kan benyttes i arbeidet med ROS-analysen, men også som et hjelpemiddel i beredskapsøvelser og i aktiviteter der sikkerhet er tema.

I en ROS-analyse settes trusselscenariene opp mot avdekte sårbarheter for å kunne vurdere risikoen knyttet til trusselscenariene samt for å vurdere hvilke sikringstiltak som bør implementeres. Det er følgelig viktig at scenarioene er både tenkelige og representative. Med representative menes her ikke *sannsynlige*, men at de beskrivelser, beslutninger og sikringstiltak man kommer frem til er basert på resultater fra disse eksemplene, og at de er relevante og dekkende for de aller fleste situasjoner som kan oppstå.[36] En god scenariobeskrivelse bør inneholde en beskrivelse av hva (hendelsesforløpet), hvem (trusselaktøren), hvorfor (hensikten) og hvordan (modus operandi/fremgangsmåte).

Under følger noen eksempler på trusselscenarier som den norske vannforsyningen kan bli utsatt for:

- **Generell kartlegging**
  En trusselaktør kartlegger vannverket og den lokale vannforsyningen gjennom åpne medier som internett, sosiale medier, kommunale arkiver m.m. samt ved å besøke områder hvor viktige deler av vannforsyningen befinner seg. Hensikten med kartleggingen er å benytte opplysningene i forberedelsene til gjennomføring av andre kriminelle handlinger som terror eller sabotasje.
- **Utro tjener/innsider**
  En utro tjener, som allerede er gitt adgang til deler eller hele vannforsyningen, stjeler, distribuerer, ødelegger eller saboterer verdier som vannverkene ønsker å beskytte.
- **Tilsiktet forurensning av drikkevannet**
  En trusselaktør forurenser drikkevannet med kjemiske, biologiske eller radiologiske substanser. Anslaget kan være rettet mot lokale drikkevannskilder, vannbehandlingsanlegg, høydebasseng eller det lokale distribusjonsnettet. Det er også mulig å tenke seg anslag rettet mot spesifikke bygninger. Scenarioet kan utføres både som et terrorangrep og som sabotasjeanslag.
- **Fysisk sabotasje av vannforsyningen**
  En trusselaktør saboterer og/eller ødelegger sentrale komponenter i den lokale vannforsyningen som vanninntak, pumpestasjoner, driftskontrollssystemer, vannbehandlingsanlegg, høydebasseng eller deler av distribusjonsnettet. Sabotasjeaksjoner kan også rette seg mot kritisk infrastruktur som strømforsyningen og telekommunikasjon. Scenarioet kan utføres både som et terrorangrep og som sabotasje av psykisk ustabile personer eller av en fremmed makt.
- **Vold og trusler benyttes for tilgang til verdier**
  En trusselaktør benytter seg av vold og trusler mot en ansatt for å få tilgang til attraktive verdier som for eksempel vannforsyningens distribusjonssystem eller driftskontrollsystem.
- **Hærverk/skadeverk**
  En trusselaktør utfører hærverk/skadeverk på deler av vannforsyningen som befinner seg lett tilgjengelig for offentligheten. Dette kan for eksempel være høydebasseng, pumpestasjoner eller i kummer som gir tilgang til deler av distribusjonsnettet.
- **Trusler om skadeverk/forgiftning**
  En trusselaktør ringer inn en bombetrusler til et vannverk eller påstår at han/hun har forgiftet drikkevannet. Trusselaktøren kan være psykisk ustabil eller ha andre grunner til ønske å skade vannverkene, kommunen eller staten.
  Det bemerkes at slike hendelser ofte vil være tomme trusler, men man må likevel undersøke saken og vurdere å foreta skadegrensende tiltak inntil saken er avklart.
- **Innbrudd med hensikt om å stjele lett omsettelig verdier**
  En trusselaktør bryter seg inn administrasjonsbygningen eller andre bygninger/anlegg/installasjoner hvor det oppbevares lett omsettelig verdier.

Denne rapporten gir nyttige råd om hvordan en kan etablere rutiner for å redusere risikoen for uønskede hendelser fra innsidere.

35) DSB definerer trusselscenario som «en detaljert og konkretisert beskrivelse av en uønsket hendelse; en beskrivelse av en fremtidig tilstand og den serien av handlinger og/eller hendelser som leder dit» Hentet fra: DSB, *Veileder til helhetlig risiko- og sårbarhetsanalyse i kommunen*, 2014, 14

36) Forsvarsbygg, *Sikringshåndboka*, 71

5. Hvordan bør vi sikre oss?

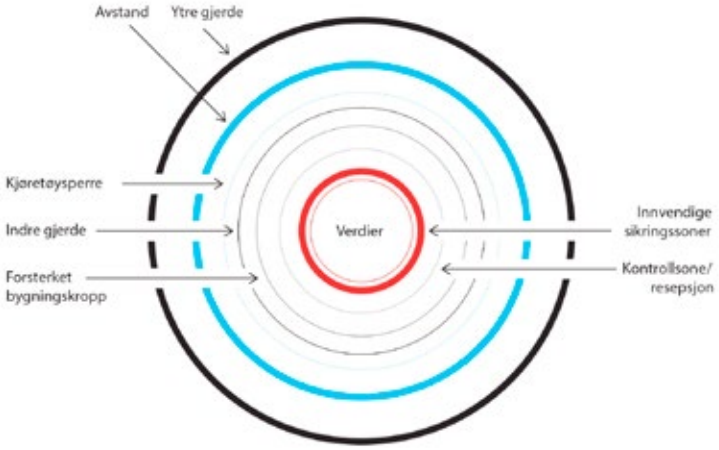
5.1. Sikringsprinsipper

Under følger en gjennomgang av noen allmenne, veletablerte prinsipper som gjelder sikring av bygg og anlegg.

5.1.1. Sikring i dybden

Sikring i dybden er et av de eldste sikringsprinsippene. Tanken bak sikring i dybden er dels å avskrekke en angriper ved at det er flere lag med sikringstiltak. Dette vil gjøre det vanskeligere og mer tidkrevende for en inntrenger å komme seg forbi sikringstiltakene, og objekteier vil da kunne vinne tid til å få på plass en utrykningsstyrke som kan settes inn for å stoppe eller begrense konsekvensene av angrepet.

Prinsippet for sikring i dybden brukes i dag både i forbindelse med utvendig perimetersikring (f. eks. gjerder, murer og kjøretøyssperrer) og innvendig sikring (f. eks. sluser ved innganger og spesielle soner rundt de viktigste verdiene inne i et bygg). Alle sikringssoner vil ha en form for fysisk forsterkning og representerer således en barriere som en inntrenger må ta seg forbi. I tillegg til de fysiske sikringstiltakene et det anbefalt å etablere vakthold, deteksjon, alarmer, adgangskontroll og kontrollrutiner i forbindelse med sonene.



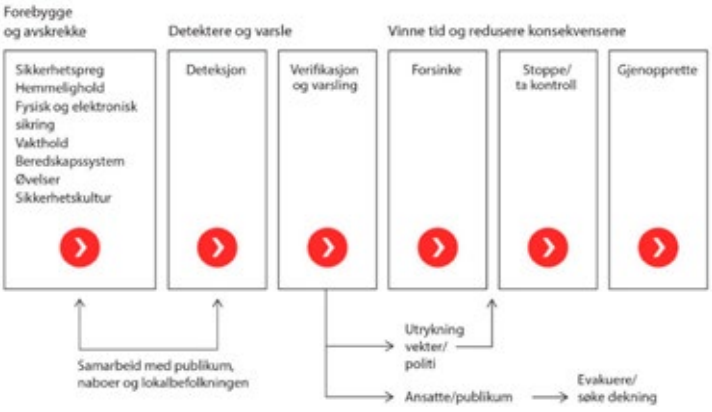
Figur 6 *illustrerer sikring i dybden med eksempler på ulike sikringstiltak som ligger lagvis utenfor verdiene. Hvert lag representerer én sikringssone. Innerst er de viktigste verdiene som vi ønsker å beskytte. Sikring i dybden innebærer at sikringstiltakene etableres i flere lag, slik at det blir vanskeligere for en inntrenger å komme forbi alle sonene og inn til verdiene. Sikring i dybden betyr at sikringstiltakene ligger lagvis innover i et areal eller volum. Tiltakene kan også være adgangskontroll, autorisasjonsskiller, dører, vegger, hvelv m.m. (Illustrasjonen er hentet fra Sikringshåndboka, utgitt av Forsvarsbygg i 2016.)*

5.1.2. Grunnsikring

Tross for at ulike sikkerhetstjenester bruker mye tid på å avdekke terroranslag, må det påregnes at det noen ganger ikke er mulig å få noen varsling i forkant av en hendelse. Vi må derfor ha en god grunnsikring som kan motstå overraskende angrep. Grunnsikringen må omfatte tiltak innenfor fysisk sikring, elektronisk og datateknisk sikring samt administrative og organisatoriske tiltak som kan håndtere potensielle trusselscenarier frem til en reaksjonsstyrke ankommer objektet. For å forsikre oss om at det er en god grunnsikring, må vi øve på håndtering av aktuelle trusselscenarier. Grunnsikringen må være tilstede permanent, og den må i tillegg være planlagt med ulike beredskapstiltak som kan forsterke sikringen ved behov. De vil spesielt være aktuelle ved ulike krisesituasjoner der det for eksempel er konflikt med en fremmed makt, og vi kan bli utsatt for målrettede sabotasjehandlinger.

5.1.3. Helhetlig tilnærming til sikring

Sikringstiltak bør fremstå som så gode og effektive at en angriper vil vurdere muligheten for å lykkes med et angrep som lav. Sikringstiltakene vil da ha en forebyggende og avskrekkende effekt. Dersom en angriper likevel forsøker seg, må vi raskt kunne detektere angrepet slik at vi kan sette inn mottiltak for å stoppe angrepet og begrense skadevirkningene.



Figur 7 *illustrerer et helhetlig sikringssystem med viktig elementer som det å forebygge, avskrekke, forsinke, detektere, verifisere, varsle, utrykning, stoppe/ta kontroll og gjenopprette. Helhetlig sikring er en videreutvikling av sikringselementene: barriere, deteksjon, verifikasjon, reaksjon og gjenoppretting. (Illustrasjonen er hentet fra Sikringshåndboka, utgitt av Forsvarsbygg i 2016.)*

Forebygge og avskrekke
Sett fra et sikringsperspektiv er det ønskelig at noen sikringstiltak er synlige for å oppnå en avskrekkende virkning. Dette må imidlertid balanseres mot behovet for å skjule sikringstiltakene for å skape overraskelse. Trusselvurderinger vil gi oss bedre kunnskap om potensielle trusler og vil være viktig for å regulere beredskapsnivået opp eller ned. Økt beredskap og øvelser innebærer i praksis en bedre sikring og vil kunne medføre at en angriper utsetter angrepet eller velger et enklere mål. Eksempler på tiltak som kan virke avskrekkende er; gjerder og skilt med advarsler, kameraovervåkning og alarmsensorer som gir økt risiko for å bli oppdaget og identifisert, avsperringer som forhindrer en trusselaktør å komme nær anlegget. Forsterket vakthold vil også kunne ha god avskrekkende effekt da dette signaliserer tilstedeværelse.

Deteksjon
Deteksjon er normalt en forutsetning for å kunne avverge et angrep. Tidlig deteksjon skaper tid og mulighet for å mobilisere aktive og passive mottiltak. Deteksjon kan utføres av ulike elektroniske sensorer (kamera, termiske kamera, bevegelsessensorer, radarer, lasere, trykksensorer og akustiske sensorer) eller mennesker (vakter, ansatte, publikum eller naboer). Ofte vil en angriper rekognosere på objektet i forkant av angrepet. Ved å gi ansatte og besøkende opplæring i å gjenkjenne mistenkelig adferd eller gjenstander, har virksomheten bedre muligheter til å detektere at et angrep er i ferd med å inntreffe. For ubemannede anlegg som ligger øde til, kan det være en god idé å alliere seg med lokalbefolkning og naboer for rapportering av uvanlige hendelser.

Verifikasjon og varsling
Ved alarm er det viktig å kunne verifisere enten med TV-overvåkning eller personell på stedet, slik at riktig reaksjon kan iverksettes. Vanligvis sender vaktsentralen ut spesielt trenede ansatte eller vaktmannskaper, eller det brukes kamera eller andre sensorer for å forsikre seg om at det er en reell alarm. Verifikasjon ved bruk av kamera er å foretrekke, slik at man unngår å sende egne ansatte eller vaktmannskaper inn i en farlig situasjon. Dersom alarmen viser seg å være reell, varsles politiet.

Forsinke
De fysiske sikringstiltakene er designet for å forsinke eller aller helst stanse en inntrenger fra å nå inn til verdier. Forsinkelsene de fysiske sikringstiltakene gir, skal også gi ansatte, besøkende og andre, mulighet til å evakuere eller rømme til sikre områder.

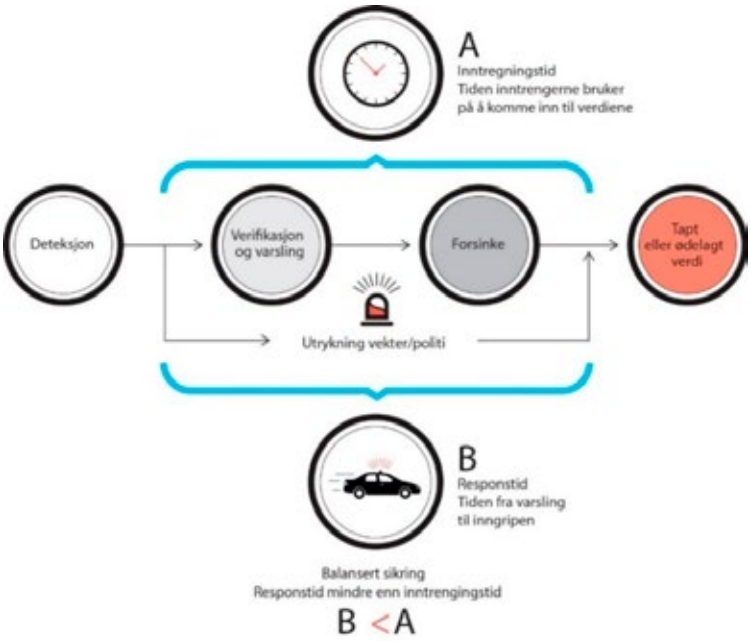
Utrykning
Utrykningsstyrken kan bestå av egne ansatte, vektere eller politi. For samfunnskritiske objekt vil det normalt være politi som rykker ut. Selv om politiets teoretisk har en kort uttrykningstid, kan andre pågående oppdrag gjøre at den reelle utrykningstiden kan bli vesentlig lengre. For å få et bedre bilde av den reelle utrykningstiden må det gjennomføres realistiske øvelser. En effektiv inngripen av politiet krever at det er tilrettelagt for dette, og at politiet er kjent på sikringsobjektet og jevnlig øver på håndtering av aktuelle trusselscenarier som kan skje på objektet.

Stoppe, ta kontroll og sikre bevis
Kommer utrykningsstyrken raskt på plass, har den mulighet til å avverge at angriperen tar seg inn på anlegget eller i bygningen, at det tas gisler eller at viktige verdier skades. Dersom responstiden er lang og/eller man har få eller svake fysiske barrierer, vil utrykningsstyrken ofte ha begrenset mulighet til å avverge en trusselsituasjon. Styrken må da fokusere på å få oversikt og ta kontroll over situasjonen ved å lokalisere inntrengere, vurdere behov for forsterkninger, evakuering og minimere skade. Det er viktig å sikre videoopptak, både som hjelp under en pågående aksjon, men også for senere etterforskning og bevisførsel.

Gjenopprette
Beredskapsplaner vil være nødvendig for å kunne håndtere spesielle hendelser og krisesituasjoner på en god måte. Alle virksomheter bør ha en plan som beskriver hvordan virksomheten skal håndtere en sikkerhetstruende hendelse. Det vil i den forbindelse være viktig å samarbeide tett med politi og redningsetatene for å få kontroll over situasjonen, redusere skadeomfanget, hindre følgeskader og rask kunne gjenopprette en tilfredsstillende tilstand. Ved en større hendelse vil det være aktuelt å etablere en krisestab. Dersom det er usikkerhet rundt om drikkevannet har blitt kontaminert vil det være nødvendig å gå ut med varsel til abbonentene. Dette vil kunne ha en betydelig skadereduserende effekt. Det er følgelig avgjørende at det etableres et eget varslingssystem for denne typen hendelse. Etter en sikkerhetstruende hendelse må det også settes ressurser for oppfølging av ansatte, andre berørte samt pårørende. Håndtering av presse vil også være viktig for å unngå å skape unødvendig frykt samt for å skjerme de som har blitt rammet og deres pårørende.

5.1.4. Balansert sikring
Balansert sikring betyr at den totale forsinkelsen de ulike sikringstiltakene gir, er større enn responstiden. Dette betyr tiden det tar få utrykningsstyrken er på plass, må

være mindre enn tiden angriperen bruker på å komme frem til verdiene eller ta kontroll over et område. Dette forutsetter at inntrengeren blir detektert og verifisert, og at størrelsen på utrykningsstyrken og bevæpningen av denne står i forhold til aktuell trusselaktør.



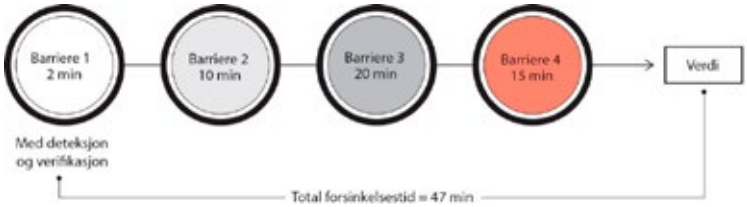
Figur 8 *illustrerer balansert sikring. (Illustrasjonen er hentet fra Sikringshåndboka, utgitt av Forsvarsbygg i 2016.)*

Tidsregnskap

For å dokumentere at man har balansert sikring, må det utarbeides et tidsregnskap. I et tidsregnskap gjør man kvalifiserte beregninger av hvor lang tid en definert trusselaktør vil bruke på å komme forbi de aktuelle fysiske sikringselementene, f.eks. gjerde, vindu, dører og vegger. En slik beregning krever kunnskap om inntrengningstider, noe man vanligvis får gjennom å gjennomføre realistiske inntrengningsforsøk eller innhenter opplysninger fra andre som har gjennomført slike forsøk.

Det er viktig å poengtere at tidsregnskap ikke er en eksakt beregning, da flere av verdiene som brukes, er basert på en subjektiv, faglig vurdering. Utrykningstid kan man relativt greit få oversikt over gjennom f.eks. møter med politiet og gjennomføring av realistiske øvelser. Kapasiteten til ulike sikringselementer mot en definert inntrenger er litt mer krevende å estimere, fordi det kan være stor forskjell på kapasiteten til en trusselaktør. Noen vil ha tilgang på toppmoderne utstyr og være godt trent, andre vil ha færre verktøy tilgjengelig.

Har man som målsetning å hindre at viktig utstyr og komponenter blir ødelagt må man ha et positivt tidsregnskap, det vil i praksis si at politiet må kunne komme til stedet å stoppe inntrengerne før de får ødelagt viktige verdier.



Figur 9 *illustrerer et tidsregnskap. (Illustrasjonen er hentet fra Sikringshåndboka, utgitt av Forsvarsbygg i 2016.)*

5.2. Metoder for sikring

Dette delkapittelet tar for seg noen metoder for sikring der sikringsprinsippene beskrevet i kapittelet over kommer til anvendelse.

5.2.1. Perimeter- og områdesikring

Perimeter- og områdesikring spiller en viktig rolle for å sikre verdiene i bygg og anlegg. I tillegg til å fungere som en klar administrativ og juridisk grense mot omverdenen er perimetersikringen det første av flere lag som bidrar til sikring i dybden og som en trusselaktør må forsere for a ta seg inn til verdiene. Slik sikring vil som oftest være både hensiktsmessig og kosteffektiv og innebærer at det etableres flere lag av fysiske barrierer og deteksjonssoner rundt verdiene som skal sikres. En godt utformet perimeter- og områdesikring vil derfor kunne bidra til å vinne tid og samtidig skape forutsetninger for egne, aktive mottiltak. Det er imidlertid viktig å være oppmerksom på at fysiske sikringstiltak i perimeteret ofte har en svært begrenset tidsforsinkende effekt for en kompetent angriper. Det bør derfor vurderes om det skal monteres sikkerhetsbelysning, alarmsensorer (innbruddsalarm) og TV-overvåkning i tilknytning til gjerdet. Normalt velger man å plassere dette innenfor gjerdet på master for å hindre at dyr utløser alarmer. Det finnes i

dag en rekke ulike kamera på markedet. Det skilles i hovedsak mellom to typer kamera:

- **Optisk** – Standard kamera. De fleste TVO-kamera gir fargebilde på dagtid og skifter automatisk til sort/hvitt på natt da dette gir bedre bildekvalitet ved dårlig belysning.
- **Termisk** – Termiske kamera «ser» den termiske strålingen (varmebølgene) fra for eksempel personer og forskjellige bakgrunner og lager et termisk bilde.

Det bør i perimetersikringen benyttes termiske kameraer til deteksjon og optiske kamera til verifikasjon. Det er ikke anbefalt å benytte optiske kamera til perimeterdeteksjon, grunnet svake presentasjoner i dårlig vær.

I tilknytning til en perimetersikring må det etablere inn- og utpasseringsmuligheter for personell og kjøretøy ved bruk av bommer og/eller porter. Portene må utformes slik at de representerer en minst like stor tidsmessig hindring for en trusselaktør som hva gjerdet som portene står i. Portene kan betjenes manuelt eller ved automatisk styring. Låsmekanismen for porter velges ut fra en vurdering av portens/bommens styrke, slik at et angrep på låsmekanismen medfører et minst tilsvarende tidstap for en innbryter som et angrep på selve porten. Ved bruk av hengelås bør minimum FG[37)] klasse 3 benyttes, i tillegg bør bøylen sitte under en stålkappe for å vanskeliggjøre kutting av låsbøylen.

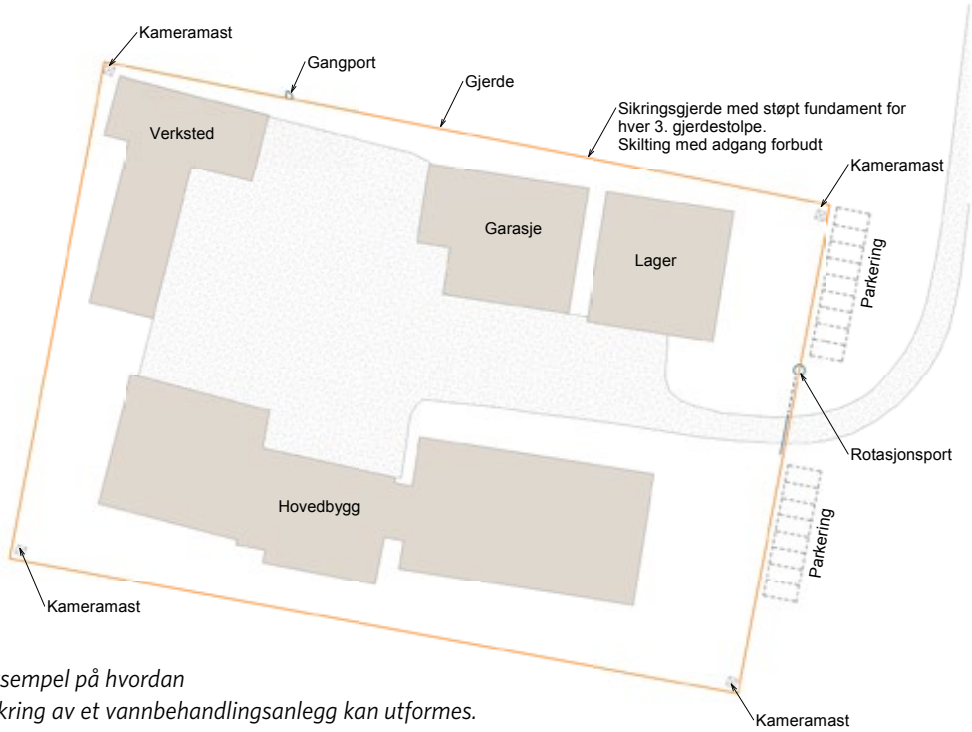
På perimeteret bør det også monteres skilt som beskriver restriksjoner i området. De fleste vil oppfatte et gjerde som et hinder som ikke skal forseres, men ved å benytte skilt forsterkes det strafferettslige vernet. Skiltene bør derfor monteres både ved inngangsportene og langs gjerdet slik at det ikke senere kan reises tvil om at ferdsel inne på område og parkering inntil gjerdet er uønsket. Skilt bør tekstes på både norsk og engelsk. Benyttes det TV-overvåkning for sikring av perimeteret skal dette angis ved egne skilt i henhold til Datatilsynets krav.

5.2.2. Skallsikring

Begrepet skallsikring brukes om sikringen av et byggets ytterste skall, altså yttervegger, tak, inngangsdører, vinduer, ventilasjonsåpninger og liknende. Hensikten med skallsikring er å etablere en sikkerhetsbarriere som søker å avskrekke og gjøre det vanskeligere for en trusselaktør å ta seg inn i bygget/anlegget.

For å oppnå en god skallsikring bør alle elementer som inngår i skallet har en tilnærmet lik fysisk styrkegrad mot definerte trusler. Det er for eksempel lite hensiktsmessig å installere en høysikkerhetsdør i en svak vegg med liten eller ingen innbruddsmotstand. I tillegg er det viktig å være oppmerksom på åpninger i skallet som kan benyttes for å ta seg inn i bygningen. Dette kan for eksempel være en ventilasjonsåpning, kabel- og rørgjennomføringer eller en kulvert. Alle åpninger større enn 30 cm i diamenter må derfor sikres tilsvarende

37) Forsikringsgodkjent



Figur 10 *Eksempel på hvordan perimetersikring av et vannbehandlingsanlegg kan utformes.*

resten av skallet for å ikke utgjøre en sårbarhet som kan utnyttes av en trusselaktør.

I tilknytning til byggets skallsikring bør det også etableres innbruddsalarmsystem som gir varsler dersom noen tar seg ulovlig inn i bygget eller anlegget. Det finnes i dag en rekke ulike sensorer som kan være aktuelle. Under følger en liste med forklaring over noen av dem:

- **Passiv infrarød detektor (PIR)** – Detekterer refleksjon av varme og gir alarm ved bevegelse i dekningsområdet.
- **Magnetkontakter** – Benyttes typisk på dører, porter, vinduer og liknende og gir alarm med åpning av for eksempel en dør.
- **Glassbruddetektor (akustisk)** – Detektoren gir alarm med skjæring og knusing av glass. Glassbruddetektoren vil ikke være like effektiv dersom det er montert film på glasset.
- **Seismisk detektor** – benyttes på betong- og stålkonstruksjoner, og gir alarm ved forsøk på skjæring, boring og sprengning på konstruksjonen. Typisk brukt på vegger, gulv, tak og dører.

I forbindelse med skallsikring bør det også vurderes å montere opp TV- overvåkningssystem for å få oversikt over situasjonen, verifisere at det er en reell alarm og for å ta opp og lagre video av hendelsen.

5.2.3. Dybdesikring/sonesikring

Også inne i et bygg eller anlegg kan det være behov for sikring. Dette kan for eksempel være et rom eller et område der det er plassert viktig utstyr som en server eller et driftskontrollsystem. Det kan også være et rom med åpne vannspeil. For å skape en ekstra barriere inn til området bør vegger, gulv, tak, dører og ventilasjonsåpninger forsterkes. Det bør også monteres et elektronisk adgangskontrollanlegg eller et nøkkelsystem for å kontrollere adgangen. I tillegg bør det etableres innbruddsalarmanlegg og vurderes om det vil være hensiktsmessig å etablere TV-overvåkning.

5.3. Sikkerhetskultur

Mattilsynet nevner i sin *Veiledning til drikkevannsforskriften* at det må etableres en god sikkerhetskultur for at de forebyggende sikringstiltakene skal ha effekt.[38] NSM definerer sikkerhetskultur som «summen av medarbeidernes kunnskap, holdninger og adferd som kommer til uttrykk gjennom virksomhetens totale sikkerhetsatferd.»[39] Forenklet kan man si at god sikkerhetskultur er når alle i en organisasjon har et bevisst og aktivt forhold til sikkerhet. Sikkerhet skal være en integrert del av alle prosesser i virksomheten, og alle må ha god nok kompetanse til å gjennomføre sine oppgaver på en hensiktsmessig måte med tanke på sikkerhet.

5.3.1. Hvorfor er god sikkerhetskultur viktig?

Den menneskelige faktoren er helt avgjørende for å ivareta sikkerheten i enhver virksomhet. Det er mennesket som skal gjennomføre virksomhetens tekniske og organisatoriske sikkerhetstiltak. Dårlig sikkerhetskultur vil derfor raskt kunne redusere effekten av kostbare fysiske og elektroniske sikringstiltak ved at de motarbeides av ansatte som ikke forstår hvorfor, eller er uenig i at de er etablert. Et typisk eksempel er at ansatte omgår sikringstiltak av «praktiske hensyn», som ved å holde en sikringsdør åpen for personen som kommer rett etter uten å sjekke at denne har riktig adgangskort. Et annet eksempel er at dører settes åpne, fordi de er tungvinte å åpne eller at ansatte selv deaktiverer alarmer.

En god sikkerhetskultur er også grunnleggende for å sikre virksomheten mot innsidetrusselen. I sine studier av innsidetrusselen i Storbritannia viser britiske *Centre for the Protection of National Infrastructure (CPNI) til at en dårlig sikkerhetskultur kan gjøre oss sårbare ovenfor en trusselaktør. Manglende årvåkenhet og etterlevelse av sikkerhetsrutiner blant ledelse og ansatte kan resultere i at mistenkelig adferd og aktivitet går ubemerket og ikke blir adressert.*[40]

5.3.2. Hvordan skape en god sikkerhetskultur?

Å bygge god sikkerhetskultur er et omfattende arbeid. Det kan være vanskelig å snu en negativ trend, og god sikkerhetskultur må være en kontinuerlig prosess. Et viktig steg på vei mot bedre sikkerhetskultur er å informere om hvilken sikring virksomheten har behov

38) Mattilsynet, *Veiledning til drikkevannsforskriften*, 2017, 17-19

39) NSM, «Sikkerhetskultur», publisert: 12.05.2014, tilgjengelig på: https://www.nsm.stat.no/om-nsm/tjenester/sikkerhetsstyring/sikkerhetskultur/

40) CPNI, «CPNI Insider Data Collection Study: Report of Main Findings», april 2013, tilgjengelig på: https://www.cpni.gov.uk/system/files/documents/63/29/insider-data-collection-study-report-of-main-findings.pdf

for, og hvorfor. Riktig sikringsnivå kan kartlegges ved å gjennomføre en risikoanalyse.

CPNI deler tiltak for å skape god sikkerhetskultur inn i to hovedkategorier: *myke* og *harde* tiltak. Mens de myke tiltakene handler om at medarbeiderne i en organisasjon skal forstå hvorfor sikringstiltak er implementert, og hvordan man utviser god sikkerhetsatferd, handler de harde tiltakene om klare retningslinjer for hva som skjer nå man utviser dårlig sikkerhetsatferd.[41)]

God sikkerhetskultur er et lederansvar

For at den enkelte ansatte skal kunne utføre sine arbeidsoppgaver med god sikkerhetsatferd, er det viktig at virksomhetens ledelse går foran som gode eksempler. Det er ledelsen som beslutter sikringstiltak som skal implementeres, og hvilke rutiner som skal være gjeldene på arbeidsplassen. Ledelsen må forklare ovenfor de ansatte hvorfor de fysiske, elektroniske og administrative tiltakene er viktige, og hvorfor de ikke skal søke å omgå implementerte tiltak av «praktiske hensyn».[42)]

Det er viktig å huske på at man ikke kan lære av sine feil dersom man ikke er klar over dem. Gode rutiner og kultur for rapportering av sikkerhetsbrudd og avvik er derfor helt avgjørende. Ved å oppfordre til rutinemessig rapportering av alle sikkerhetsbrudd, kommuniserer virksomheten at sikkerhet blir tatt på alvor. Samtidig skapets bevissthet og mulighet for diskusjon rundt sikkerhetssituasjonen og forbedringstiltak. Det er også viktig å huske på hvilke forutsetninger de enkelte ansatte har, spesielt med tanke på opplæring. En person kan ikke lastes for de feil han eller hun begår hvis det ikke har blitt gitt tilstrekkelig opplæring. Det er de ansatte som kjenner egen arbeidsplass best, og det er derfor lurt at de opplæres i hvordan de skal reagere og varsle ved mistenkelig adferd. Årvåkne ansatte kan ofte enklere identifisere adferd som strider mot det normale, enn det vaktpersonell har mulighet til å gjøre gjennom videoovervåkning og vaktrunder. Disse har ansvar for mange objekter og det vil være vanskeligere for dem å skille unormal aktivitet fra det normale i en virksomhet.

De harde tiltakene handler om å skape rutiner for å håndtere dårlig sikkerhetsatferd. Det skal være klare retningslinjer for hvordan oppgaver skal utføres på en sikkerhetsmessig tilfredsstillende måte, og retningslinjene må håndheves på en synlig og effektiv måte. Det må kommuniseres tydelig til medarbeiderne at dårlig sikkerhetsatferd får konsekvenser, og at det forventes at retningslinjene etterleves.[43)]

Følgende tiltak anbefales for å forbedre sikkerhetskulturen:

- Ledelsen må ha fokus på sikkerhet og fremheve at sikkerhet er viktig
- Generell opplæring av alle ansatte med tanke på sikkerhetsrutiner og sikkerhetsbrudd
- Obligatoriske opplæringspakker, f.eks. ved bruk av e-læring med avsluttende test for å kontrollere at man har oppnådd et tilfredsstillende kunnskapsnivå
- Informasjon om implementerte fysiske og elektroniske sikringstiltak
- Bevisstgjøring rundt hva som utgjør sensitiv og skjermingsverdig informasjon
- Bevisstgjøring rundt hvordan ulik type informasjon skal oppbevares eller behandles
- Utarbeidelse av planverk og instrukser for sikkerhetstruende hendelser
- Øve på håndtering av sikkerhetstruende hendelser og evakuering
- Fokus på trusselscenarier og årvåkenhet ovenfor mistenkelig adferd, inkludert innsidetrusselen
- Innføring av rapporteringssystem for sikkerhet og oppfølging av ansatte som rapporterer om brudd

Oppsummert handler en god sikkerhetskultur om å bevisstgjøre og motivere de ansatte til god sikkerhetsatferd. Rapportering av sikkerhetsbrudd og oppfølging av disse må ikke handle om å henge ut personer for de feilene man har gjort, men om å skape systemer og rutiner som fanger opp og retter opp i dårlig sikkerhetsatferd. Feil bruk av rapporteringssystemer kan føre til at færre ønsker å melde inn sine observasjoner og at virksomheten på denne måten får et skjevt bilde av den reelle sikkerhetssituasjonen.

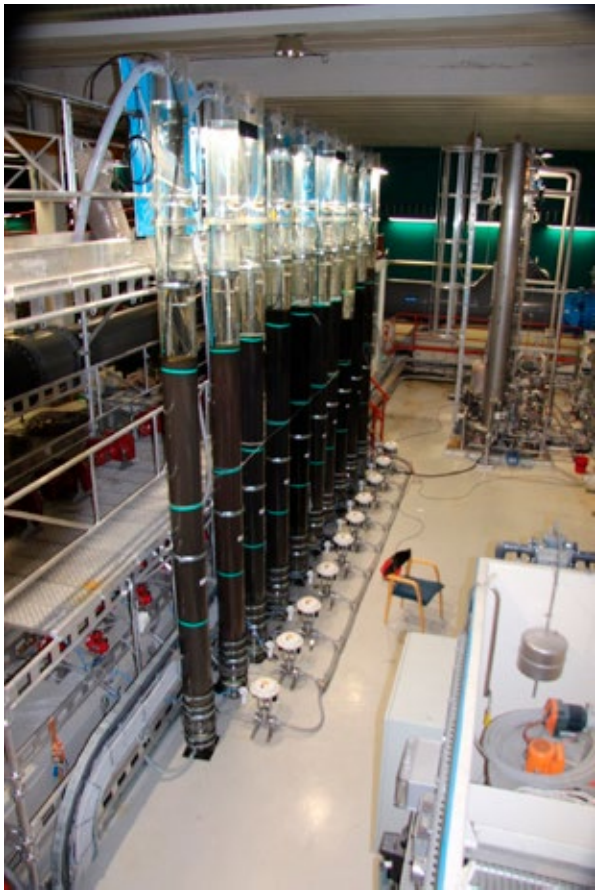
Uavhengig av metode krever det at ledelsen går foran som et godt eksempel og setter krav til at rutiner følges. Ledelsen må arbeide kontinuerlig med å skape bevisstgjøring og årvåkenhet, og hele virksomheten må være med på øvelser.

41) CPNI, «Board Security Passport», publisert: 2017, tilgjengelig på: https://www.cpni.gov.uk/content/good-governance

42) NSM, «Hvordan skape en god sikkerhetskultur?», publisert: 17.06.2014, tilgjengelig på: https://www.nsm.stat.no/om-nsm/tjenester/sikkerhetsstyring/sikkerhetskultur/hvordan-skape-en-god-sikkerhetskultur/

43) CPNI, «Board Security Passport», publisert: 2017, tilgjengelig på: https://www.cpni.gov.uk/content/good-governance

For å lykkes med å skape og opprettholde en god sikkerhetskultur anbefales en helhetlig tilnærming og samarbeid på tvers av avdelingene i virksomheten. På denne måten kan virksomheten få frem det fulle potensialet i både medarbeidere og i de fysiske og elektroniske sikringstiltakene som etableres.[44)]



Noen vannverk har bygd egne anlegg som benyttes til forsøk og visualisering av behandlingsprosessen. Dermed trenger man ikke å ta med besøkende inn i selve vannverket. Bildet viser IVAR's pilotanlegg på Langevatn.

44) For mer om hvordan en god sikkerhetskultur oppnås, se: Forsvarsbygg, *Sikringshåndboka*, 2016

6. Hvordan sikrer vi oss i praksis?

Det finnes i dag flere tusen vannverk i Norge. Disse vannverkene strekker seg fra å være små, private vannverk som kun forsyner mindre tettsteder til å være store offentlige vannverk som forsyner over 100 000 abonnenter med vann. Det enkelte vannverk er her ansvarlig for hele vannforsyningsprosessen – altså fra vannet blir hentet fra vanntilsigsområdet/kilden, rensing av vannet i vannbehandlingsanleggene til distribuering av vann ut til forbruker. Dette kapittelet skal ta for seg hvordan man rent praktisk kan gå frem for å sikre vannforsyningen og de ulike delene som inngår i vannforsyningen.

6.1. Planlegging og gjennomføring av sikringsprosjekter

6.1.1. Planleggingsgrunnlag for sikring

Drikkevannsforskriftens § 10 stiller krav om at vannbehandlingsanlegg og alle relevante deler av distribusjonssystemet skal være tilstrekkelig sikret. Hvilke deler av vannforsyningssystemet som er relevante å sikre og hva som anses som tilstrekkelig må imidlertid vurderes for hvert enkelt vannforsyningssystem.[45)] Grunnen til dette er at ulike vannforsyningssystem og ulike deler av forsyningen kan stå ovenfor ulike trusler og trusselaktører avhengig av forhold som for eksempel sårbarhet, størrelse, beliggenhet eller samfunnskritiske abonnenter.

For enhver virksomhet er det en utfordrende oppgave å vurdere hvilke verdier de skal beskytte, hvilke mulige trusler de står ovenfor, hvor sårbare de er ovenfor truslene, og hvilken risiko de bør håndtere i fremtiden. Risiko- og sårbarhetsanalysen (ROS) er et metodisk verktøy som er utarbeidet blant annet for å hjelpe virksomheter å besvare disse spørsmålene på best mulig måte. I *Veiledning til drikkevannsforskriften* stiller Mattilsynet krav om at det skal ligge en helhetlig risiko- og sårbarhetsanalyse til grunn for vannverkenes beredskapsplanverk. [46)] En slik analyse bør også brukes for å vurdere hva som er tilstrekkelig sikring for det enkelte vannverk.

I ROS-analysen vurderes hvilke verdier en virksomhet har, sårbarheten disse verdiene har ovenfor et sett med utvalgte trusselscenarier, risikobildet og hvordan man kan håndtere risiko ved hjelp av ulike tiltak. En slik analyse vil gi vannverkene en oversikt over risikobildet de står ovenfor og dermed være et nyttig verktøy for å vurdere hva som skal sikres, hvordan det enkelte vannforsyningssystemet skal sikres og hva som kan anses som tilstrekkelig sikring mot de trusselene som er avdekket i analysen. ROS-analysen vil også være et nyttig verktøy som kan benyttes til å vurdere og sammenlikne ulike alternativer for sikringsløsninger.

For at vannverkene skal få dannet seg et best mulig risikobilde anbefales at det gjennomføres en egen separat ROS-analyse for tilsiktede uønskede handlinger (security). Det er fordi det er vesentlige forskjeller mellom security-hendelser (terror, sabotasje, etterretning og annen kriminalitet) og det som gjerne blir omtalt som safety-hendelser (ulykkeshendelser, naturkatastrofer eller teknisk svikt) Se side 12.
Som følger av at security-hendelser er knyttet til en strategisk aktør, som blant annet ikke ønsker å avdekke sin handlingsplan forut for angrepet og som ved hjelp av «menneskelig oppfinnsomhet» kan omgå etablerte sikringstiltak, er det knyttet stor usikkerhet til slike hendelser.[47)] Sammenliknet med safety-hendelser er også datagrunnlaget for security-hendelser svakere. Dersom safety- og security-relaterte hendelser blir behandlet i en og samme analyse risikerer man derfor at security-hendelsene vil komme ut med *lav* sannsynlighet, mens safety-hendelsene kommer ut med *moderat* eller *høy* risiko. Dersom man ikke er bevisst dette kan det resultere i at sikringstiltak rettet mot security-hendelser blir nedprioritert.[48)]

Det er vannverkene selv som må ta stilling til hva de anser for å være akseptabel risiko. Trusselscenarier med uakseptabel risiko kan håndteres med ulike strategier

45) Mattilsynet, *Veiledning til drikkevannsforskriften*, 2017-17-19

46) Mattilsynet, *Veiledning til drikkevannsforskriften*, 2017, 17-19

47) Jore, «Safety and Security – is there a need for an integrated approach?», 855-856 og Smith, C. og D. Brooks, *Security science. The therory and Practice of security*, Oxford: Elsevier, 2013, 9

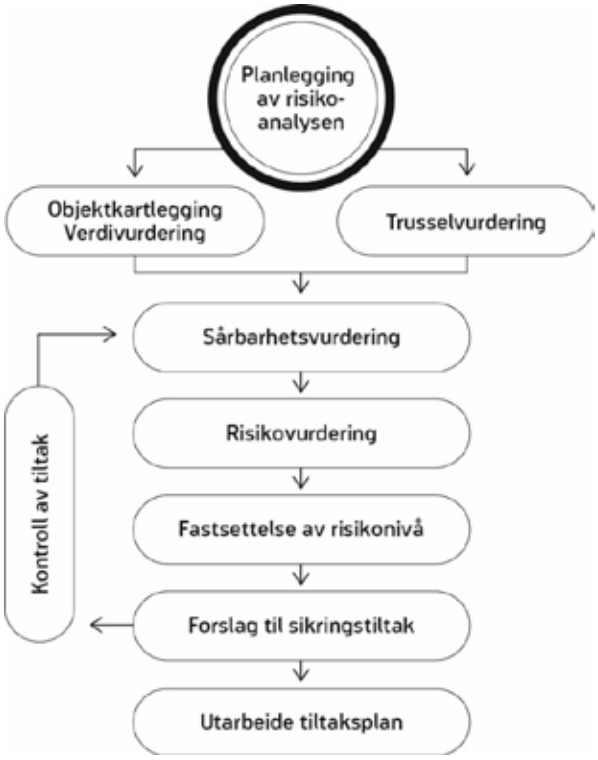
48) Jore og Egeli, «Risk management methodology for protecting against malicous acts – are probabilites adequate means for describing terrorisme and other security risks?», 812 og Busmundrud m.fl., *FFI-rapport 2015/00923 Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger*

som å unngå, overføre, akseptere eller redusere risiko. I mange tilfelles vil det simpelthen ikke være mulig å unngå eller overføre risiko, da står valget mellom å akseptere eller redusere risiko. Å redusere risiko handler om å iverksette sikringstiltak som vil redusere konsekvensene, sårbarhetene og/eller sannsynligheten for at et trusselscenario inntreffer.

6.1.2. Gjennomføring av risiko- og sårbarhetsanalyse

Det finnes flere metoder som kan benyttes for å gjennomføre en risiko- og sårbarhetsanalyse med hensyn på tilsiktede uønskede handlinger (security). I Norge er det i hovedsak tre standarder som bidrar til denne prosessen. Herunder *ISO 31000 Risikostyring og retningslinjer, NS5814:2008 Krav til risikovurderinger og NS5832:2014 Samfunnssikkerhet – Beskyttelse mot utilsiktede uønskede handlinger – Krav til risikoanalyse.* For gjennomføring av risikoanalyse er det utarbeidet en rekke ulike veiledere som kan være nyttige for vannverkene i utarbeidelsen av ROS-analyser. Her kan nevnes:

- Mattilsynet, «Veiledning i økt sikkerhet og beredskap i vannforsyningen – fra ROS til operativ beredskap», 2017
- DSB, Veileder til helhetlig ROS i kommunen, 2014
- NSM, Veiledning i risiko- og sårbarhetsanalyse, 2006



Figur 11 *Forsvarsbyggs modell for gjennomføring av risikoanalyse av villede (kilde Sikringshåndboka 2016)*

I tillegg har Norsk Vann gitt ut en rapport om sikkerhetsstyring i vannbransjen. Denne rapporten inneholder også noe informasjon om risikoanalyse.[49)]

I dette delkapittelet vil det gis noen generelle råd og tips til hvordan vannverkene kan gjennomføre en ROS-analyse. Disse rådene kan brukes som et supplement til de overnevnte veilederne.

Planlegging av risikoanalysen

Ethvert prosjekt bør ha en planleggingsfase. Denne fasen av prosjektet innebærer å avklare behov, lære opp nøkkelpersonell og etablere prosjektgrupper av relevante personer. Det er viktig å sette av tilstrekkelig med tid i planlegging av risikoanalysen. De mest sentrale delene av planleggingsfasen er følgende:

- Valg av metode
- Målsetninger og forventinger
- Ledelsesforankring
- Fastsette risikokriterier og sikringsmål
- Datainnsamling
- Organisering av prosjektgrupper
- Resultatene fra analysearbeidet bør dokumenteres

Objektkartlegging og verdivurdering

Objektkartlegging er en beskrivelse av analyseobjektet, ofte kalt systembeskrivelse. Objektet skal kartlegges, herunder oppdrag, organisasjon, beliggenhet, bygningsmasse, infrastruktur, fysisk og elektronisk sikring og administrative rutiner. En inndeling av objektet etter lag-på-lag-prinsippet kan være en fordel for en god beskrivelse av objektet med sikringstiltak. Objektkartleggingen bør også gjengi organisering, verdikartlegging og virksomhetens formål. En kartlegging kan med fordel inkludere:

- Administrative forhold
- Sikkerhetsorganisasjon
- Verdivurdering
- Omkringliggende områder
- Beskrivelse av objektet med sikringstiltak
- Vakt og reaksjonsapparat

Relevante tegninger og kart bør benyttes som grunnlag i planleggingsfasen og ved befaring. Verdiene bør defineres i forkant av befaringen, og bør være utgangspunkt for kartleggingen. Det er en fordel å dokumentere befaringen med bilder og notater som kan benyttes senere i analysearbeidet.

For mer om verdivurdering se delkapittel *3.1 Verdi- og skadevurdering*.

49) Norsk vann, *Sikkerhetsstyring for vannbransjen*, Norsk vann-rapport: 213/2015

Trusselvurdering

Trusselvurderingen er en kartlegging av det nåværende trusselbildet. Som kilder kan både åpne og graderte trusselvurderingen for eksempel fra PST, NSM og E-tjenesten benyttes. Det er også relevant å benytte seg av statistikk fra Statistisk sentralbyrå, tidligere sikkerhetstruende hendelser i virksomheten samt rapporter om kriminalitet. I trusselvurderingen deles truslene inn i fire ulike kategorier: etterretning, terrorisme, sabotasje og annen kriminalitet. Innen disse kategoriene gis en generell beskrivelse av den nåværende trusselsituasjonen, aktuelle aktører og deres arbeidsmetode.
Basert på trusselvurderingen utarbeides trusselscenarier som eksempler på hva som kan skje. En scenariobeskrivelse bør inneholde en beskrivelse av *hva* (hendelse), *hvem* (trusselaktør), *hvorfor* (hensikten) og *hvordan* (modus operandi). I risikoanalysen brukes trusselscenariene til å vurdere sårbarhet og risiko som den enkelte virksomhet står ovenfor.

Sårbarhetsvurdering

En sentral del av risiko- og sårbarhetsanalysen er sårbarhetsvurderingen. Sårbarhetsutvalget definerte sårbarhet som «de problemer et system vil få med å fungere når det utsettes for en uønsket hendelse, samt de problemer systemet får med å gjenoppta sin virksomhet etter at hendelsen har inntruffet.» [50)]
Systemet vil i denne sammenheng være vannforsyningen.

Sårbarhet er således en iboende svakhet ved et objekt eller et system. For å finne disse er man avhengig av svært god kunskap om alle objektet deler og avhengigheter. Når vi skal vurdere sårbarheter så gjøres det med utgangspunkt i trusselscenarioene og de eksiterende sikringstiltakene.

50) NOU 2000: 24 Et sårbart samfunn — Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet, 18

Sårbarhet	Beskrivelse
Lav	Eksisterende sikringstiltak er effektive og vil i stor grad motstå en uønsket hendelse
Moderat	Eksisterende sikringstiltak er effektive, men er noe mangelfulle
Høy	Eksisterende sikringstiltak er lite effektive og mangelfulle
Svært høy	Det eksisterer ingen spesielle sikringstiltak

Figur 12 *Eksempel på tabell for klassifisering av sårbarhet.*

Risikovurdering og fastsettelse av risikonivå

I denne delen av analysen sammenstilles resultatene fra verdi, trussel og sårbarhetsvurderingen. Dette gjøre for alle trusselscenariene. Risikoen vurderes etter fastsatte kriterier, som vil variere etter hvilken standard som benyttes.

Etter NS 5814 *Sannsynlighet og konsekvens* vurderes sammenhengen mellom identifiserte konsekvenser (skade/tap av verdi) og sannsynligheten (trusler og sårbarheter). Arbeidsgruppen diskuterer seg frem til samlet risiko for det enkelte scenario ved å gjøre en kvalitativ vurdering av sannsynlighet og konsekvens etter gitte kriterier. Risikoen uttrykkes altså som forholdet mellom sannsynlighet og konsekvens. Det bør benyttes et konsekvensskjema som angir konsekvensen ved tap av verdien. Det bør også utarbeides kriterier for vurdering av konsekvens, fordelt på de ulike kategoriene (a) operativ evne/drift, (b) sensitiv informasjon, (c) liv og helse og (d) økonomiske konsekvenser. For vannverkene kan det også være aktuelt å vurdere omdømme som en egen kategori.

Også i sannsynlighetsvurderingen må det benyttes noen kriterier for å bestemme grad av sannsynlighet i hvert **enkelt** scenario. Dette er en subjektiv vurdering der sannsynlighet vurderes på en skala fra 1 (LAV) til 5 (SVÆRT HØY). Sannsynlighet vurderes etter følgende kriterier:

- Tilstedeværelse av verdi
- Trusselaktørens intensjon og kapasitet
- Fravær av aktive og passive sikringstiltak
- Historiske data
- Trendrapporter

Trusselaktørens mulighet til å ødelegge, ta bort eller forringe verdiene vurderes for hvert enkelt trusselscenario.

Risikoen for de ulike trusselaktørene kan presenteres i form av en risikomatrise, for eksempel en Boston Square Matrix. I analysen settes det opp en matrise per konsekvensklasse (liv og helse, operativ evne, økonomi og informasjon).

Etter NS5832 *Trefaktormodellen* beskrives risikoen som forholdet mellom verdi, trussel og sårbarhet. Risikoen rangeres etter fastsatte kriterier som er tilpasset virksomhetens egenart, og kan presenteres på forskjellig måter. NSMs *Håndbok: Risikovurdering for sikring* gir råd til virksomheter om hvordan denne typen risikoanalyser kan planlegges og gjennomføres.[51)]

6.1.3. Stategier for å håntere risiko (ACAT)

Det finnes ulike strategier for å håndtere risiko. ACAT er en kjent strategi for håndtering av risiko, hvorav de fire bokstavene står for *Avoid*, *Control, Accept og Transfer*. Dersom denne strategien benyttes, kan man utfra ulike risikoer benytte en eller flere strategier for å håndtere risiko:

- Unngå (Avoid): Aktiviteter som innebære risiko, unngås av virksomheten. Et eksempel kan være å ikke benytte seg av foreslått tomt for utbygging fordi dette innebærer en for stor risiko.
- Redusere (Control): Iverksette tiltak for å redusere sannsynligheten eller konsekvensen av en tilsiktet hendelse. Tiltak kan være for eksempel fysiske eller organisatoriske sikringstiltak.
- Aksept (Acceptance): Akseptere konsekvensen som en følger av en tilsiktet hendelse. Dette inkluderer tilsiktede hendelser som har katastrofale konsekvenser, men der man anser muligheten for at dette skal skje, som meget lav. Da vil man kunne vurdere at kost-nytte tilsier at det ikke er økonomisk forsvarlig å sikre seg mot alle tenkelige tilsiktede hendelser.
- Overføring (Transfer): Overføre risikoen til en annen virksomhet, annen lokasjon eller en annen avdeling. Dette kan for eksempel være en verdi som kan flyttes til en annen lokasjon med bedre grunnsikring eller at man outsorcer deler av virksomhetens oppgaver til et annet selskap.

De mest aktuelle sikringsstrategiene for vannforsyningen vil trolig være *reduksjon og aksept*..

6.1.4. Planlegging av sikringsløsninger

For å få gode sikringsløsninger i et prosjekt er det viktig at sikkerhet settes på dagorden på et tidlig i prosjektplanleggingen. Det må avklares hvilke forventinger og behov man har. Sikkerhet en kun et av mange aspekter som skal ivaretas et byggeprosjekt, og en bevissthet rundt sikkerhet hos oppdragsgiver og byggherre, arkitekter og rådgivende ingeniører kan bidra til gode løsninger som forener ulike interesser.

Det kan være både utfordrende og kostbart å sikre et eksisterende bygg. Dette gjelder spesielt der det eksisterende sikringsnivået er lavt. Det kan derfor være nødvendig å etablere en langsikring plan for å gjennomføre nødvendige sikringstiltak.

Ved sikring av et eksisterende bygg er det viktig å se helheten og ha kunnskap om de ulike bygningselementene. Dette for å sikre at man for eksempel ikke setter inn en kraftig sikkerhetsdør i en vegg med liten motstandskraft mot inntrengning. I ubemannende bygg er det ofte mange usikrede vinduer som kan utgjør en stor sårbarhet med tanke på inntregning. I stedet for å sette inn et sikkerhetsvindu kan man vurdere om det er mulig å støpe igjen vinduså̊pningen. Sikring av eksisterende ytterdører kan gjøres med ulike forsterkningstiltak som for eksempel, rullegitter, bommer eller ekstra låsing. En utfordring er imidlertid at man ikke helt vet kapasiteten til den forsterkede døren med mindre man gjennomfører en innbruddstest. Det sikreste alternativet, men ofte det mest kostbare vil være bytte ut døren med en godkjent sikkerhetsdør testet etter Norsk standard EN 1627 *Dører, vinduer, påhengsvegger, gitter og skodder. Innbruddssikkerhet. Krav og klassifisering* utgitt av Standard Norge.[52)].

6.1.5. Beskyttelse av sensitiv informasjon

Åpenhet er et svært viktig prinsipp i offentlig saksbehandling, men for samfunnskritisk infrastruktur som drikkevannsforsyningen må åpenhet veies opp mot behovet for å skjerme informasjon av sikkerhetsmessig årsaker. Dette for å unngå at informasjonen misbrukes til for eksempel å planlegge et angrep mot vannforsyningen. Sensitive opplysninger, tegninger, tekniske beskrivelser, kart med mer bør derfor sikres og behandles slik at *kun* de med tjenstlig behov får tilgang på informasjonen. Dette kalles på engelsk «need-to-know» -prinsippet, og må gjelde både for kunder, leverandører, konsulenterog egne ansatte.

Hvilken konkret informasjon som bør skjermes må være opp til en vurdering av den enkelte vannverkseier. Opplysninger om sårbarheter og sikringstiltak knyttet til vannforsyningen er imidlertid eksempler på informasjon som bør skjermes. Spesielt ved bygging av nye bygg og anlegg og ved utførelsen av vedlikeholdsarbeider på eksisterende bygningsmasse er det viktig å definere hva

51) Mattilsynet, *Veiledning i økt sikkerhet og beredskap i vannforsyningen – fra ROS til operativ beredskap, 2017*

52) Tilgjengelig på: https://www.standard.no/

som er sensitiv informasjon. Også oversiktskart over hele vannforsyningens ledningsnett bør skjermes. Ved behov, for eksempel i forbindelser med gravearbeider, kan imidlertid utsnitt av disse kartene deles. Da bør det imidlertid registerets hvilke kart som blir distribuert og til hvem. For samfunnskritiske abonnenter som for eksempel skjermingsverdige objekter, bør vannverkene gå i dialog med objekteier og vurdere hvorvidt informasjon om kummer og inntaksledninger er skjermet tilfredsstillende. Det bør også tas en gjennomgang av informasjonen om vannforsyningen som er lagt ut på nettet i dag, både av vannverket og av leverandører, slik at eventuell sensitiv informasjon kan slettes. I 2016 oppdaget f eks NVE at sensitiv informasjon om kraftforsyningen lå ute på internett.[53)]

For at alle som blir gitt informasjonen skal være oppmerksom på at den er sensitiv bør den merkes. Vannverkseiere som ikke er omfattet av sikkerhetsloven kan ta i bruk Offentleghetslova og merke dokumentet med *Unntatt Offentligheten* § 21 eller §24.3[54)] eller Beskyttelsesinstruksens beskyttelsesgrader: *Fortrolig eller Strengt Fortrolig*[55)]. I tillegg til bør eiere, ansatte, leverandører og konsulenter som har behov for tilgang til sensitiv informasjon undertegne en taushetserklæring. I taushetserklæringen forplikter vedkommende seg til å ikke dele sensitiv informasjon med andre både mens de er ansatt/engasjert og etter at ansettelsesforholdet eller oppdraget er avsluttet.
Rapport 238 fra Norsk Vann som utgis våren 2018 vil grundig behandle temaet *informasjonssikkerhet*.

53) *https://www.tu.no/artikler/statnett-ropet-hemmelig-informasjon-om-det-norske-kraftsystemet/366395*

54) *Lov om rett til innsyn i dokument i offentleg verksemd (offentleglova)* og *Instruks for behandling av dokumenter som trenger beskyttelse av andre grunner enn nevnt i sikkerhetsloven med forskrifter (beskyttelsesinstruksen) § 21 omhandler unntak fra innsyn blant annet pga. nasjonale trygghetshensyn, mens § 23.1 omhandler unntak fra innsyn for opplysninger når unntak er påkrevd fordi innsyn ville lette gjennomføringen av straffbare handlinger*

55) Beskyttelsesinstruksen er tilgjengelig på: http://www.lovdata.no

6.2. Sikring av ulike delene av vannforsyningen

For at vannforsyningen skal sikres på en tilfredsstillende måte bør det etableres en god grunnsikring for alle norske vannforsyningssystemer. En god og helhetlig grunnsikring omfatter tiltak innenfor fysisk sikring, elektronisk sikring samt administrative og organisatoriske tiltak. Disse tiltakene bør bestå av en kombinasjon av barrierer, deteksjon, verifikasjon og reaksjon som er tilpasset det enkelte vannforsyningssystemet.

Det er ikke mulig å gi en detaljert beskrivelse av en grunnsikring som kan implementeres på alle norske vannforsyningssystemer. Dette skyldes store variasjoner i både design og byggemåte, så vel som at de ulike forsyningssystemene står ovenfor ulike sikringsproblemstillinger blant annet som følge av beliggenhet, størrelse og andre lokale forhold. Både grunnsikring og eventuell tilleggssikring må derfor utarbeides på grunnlag av en egen ROS-analyse og med utgangspunkt i sikringsprinsippene som har blitt beskrevet i denne veilederen.

I de etterfølgende delkapitlene vil det likevel gjøres et forsøk på å gi en overordnet beskrivelse av grunnsikringen av de ulike bestanddelene av vannforsyningen. Det vil også trekkes frem noen gode løsninger i form av bilder og skisser. Dette gjøres for å gi vannverkene en bedre forståelse av hva som anses som en god grunnsikring. Listen over grunnsikringstiltak er imidlertid ikke uttømmende og den skal *ikke* brukes som erstatning for en ROS-analyse.

For hver enkelt bestanddel beskrives et grunnsikringsnivå og tilleggssikring Vannverkene bør i et lengre tidsperspektiv forsøke å tilfredsstille grunnsikringsnivået. Det er ROS-analysen som må avgjøre hvorvidt tilleggssikringen også bør implementeres.
For etablering av grunnsikring for nye bygg vises det til delkapittel *6.2.7 Nybygg*.

6.2.1. Vannkilde (overflatevann)

Dette delkapittelet vil ta for seg overflatevann, mens grunnvannskilder/brønner vil bli behandlet sammen med råvannsinntaket i delkapittel *6.2.2 Bygg eller annen installasjon for grunnvannskilder og råvannsinntak.*
Det kan være umulig eller svært utfordrende å sikre overflatevann som en innsjø eller en elv mot at uønskede får tilgang til kilden. Dette følger av forhold som blant annet størrelse og beliggenhet. Hvorvidt det skal etableres sikringstiltak rundt vannkilden eller om

vannverket velger å akseptere risikoen, bør derfor vurderes med utgangspunkt i en ROS-analyse.

Når det gjelder forurensning/forgiftning av en vannkilde vil skadeomfanget variere etter forhold som vannvolum, tilgjengelighet til vannkilden og plasseringen av vanninntaket. Dette følger blant annet av at jo større vannvolum, desto større mengde trusselstoffer er nødvendig for å forurense kilden.[56] Oppsummert er det viktig at følgende punkter vurderes i ROS-analyse:

- Beliggenhet
- Volum
- Tilgjengelighet/fremkommelighet
- Plasseringen av vanninntak
- Andre lokale forhold som er relevante

Utfordringene ved å etablere en tilstrekkelig god fysisk og elektronisk sikring rundt vannkilden gjør at de menneskelige og organisatoriske tiltakene blir desto viktigere. Et sentralt sikringstiltak vil være å sørge for at sensitive opplysninger ikke kommer på avveie. Det er følgelig viktig å etablere en god sikkerhetskultur i vannverkene og arbeide med bevisstgjøring av hva som er sensitiv informasjon og hvordan dette skal behandles og oppbevares.

Dersom trusselscenariene som omhandler angrep mot vannkilden kommer ut med uakseptabelt høy risiko i ROS-analysen må det iverksettes ytterligere tiltak. Det vil være da være avgjørende å etablere en form for deteksjonstiltak som sørger for at angrepet detekteres og at skadereduserende tiltak kan iverksettes. For mindre vannkilder kan det også være aktuelt å etablere ferdselsrestriksjoner og TV-overvåkning av kilden. Dersom det også vurderes som hensiktsmessig å begrense tilgangen til kilden kan det være aktuelt å etablere fysiske sikringstiltak som kjøretøyssperrer og eventuelt gjerder i avgrensede områder hvor det er hyppig ferdsel. All merking av vanninntak med bøyer o.l. bør fjernes for å gjøre det vanskeligere å finne eksakt plassering av vanninntak. Et skadereduserende tiltak dersom en slik hendelse skulle inntreffe er å ta i bruk reservevannkilder og/eller vannforsyningen til nabokommunen.

56) Lia og Nesser, «Terror mot drikkevann», 17

Grunnsikring	**Forebygging, deteksjon og verifikasjon** ▪ All merking av vanninntak med bøyer og lignende bør fjernes. *Elektronisk sikring:* ▪ For mindre vannkilder kan det vurderes om det er hensiktsmessig å etablere TVO-kamera slik at man kan overvåke vannkilden og/eller vanninntaket. Kamerabildene overføres til et alarmmottak/ driftssentral. **Reaksjon** *Vakt- og reaksjonsstyrke/Varslingssystemer* ▪ Varsling av abonnenter og lokalbefolkningen iht. beredskapsplan og etter dialog med helse- og tilsynsmyndigheter, dersom det er usikkerhet rundt om drikkevannet er forurenset/forgiftet. **Gjenoppretting** *Redundans* ▪ Den lokale vannforsyningen bør kobles opp til en reservevannkilde eller vannforsyningen i nabokommunen.
Tilleggs-sikring	**Barrierer** *Perimetersikring:* ▪ Det bør vurderes om det er hensiktsmessig å etablere kjøretøyssperrer/bommer og/eller andre sperrer for å begrense muligheten for kjøretøy skal kunne komme helt fram til vannkilden.

Figur 13: *Beskrivelse av grunnsikring og tilleggssikring for vannkilder (overflatevann).*

6.2.2. Bygg eller annen installasjon for grunnvannskilde og råvannsinntak

Råvannsinntaket består gjerne av et bygg eller annen installasjon med inntaksrør, fordelingsrør og pumper. Bygget kan være utført i både betong og murverk, men de fleste av de eksisterende byggene er utført i trevirke og kun utstyrt med enkle dører og vinduer uten spesiell sikring. Det samme gjelder bygg/installasjoner hvor grunnvannskilden eller brønnen befinner seg.

For å forsterke skallsikringen på slike bygg/installasjoner kan man ta i bruk stålplater og kryssfiner samt bytte ut eksisterende dører med sikkerhetsdører med FG-godkjente låser eller montere rullegitter foran dører/porter. Der anlegget er ubemannet bør det vurderes å kle igjen/støpe igjen vinduene. Alternativt kan vinduene sikres med sikkerhetsgodkjent gitter. Disse fysiske sikringstiltakene vil både kunne virke avskrekkende og forlenge trusselaktørens inntrengningstid noe.

En forsterkning av skallsikring i bygg med trevegger kan imidlertid være både omfattende og kostbar. Dersom forsterkning av den eksisterende skallsikring ikke er mulig å gjennomføre, eller en kost- og nytteanalyse viser at en slik forsterkning ikke vil være hensiktsmessig anbefales at det etableres kompenserende tiltak. Et slikt tiltak kan være å etablere et perimetergjerde rundt eiendommen. Utstyrt med skilt med advarsler vil gjerde både kunne markere en juridisk grense rundt bygget og virke avskrekkende. Det vil også kunne utgjøre en fysisk barriere mot mindre avanserte trusselaktører som for eksempel ungdom som gjør hærverk.

Fysiske sikringstiltak vil imidlertid ha en begrenset betydning dersom det ikke også etableres noen form for deteksjon- og verifikasjonstiltak. Dette kan gjøres ved etablering av innbruddsalarm inne i bygget/installasjonen eller ved at det etableres termiske og optiske kamera på bygget utside. Dersom det ikke er mulig med overføring av kamerabilder til alarmmottak/driftssentral bør det etableres rutiner for at vekter/ansatt responderer på utløste alarmer. Det er imidlertid viktig å bemerke at dersom det er mistanke om noe kriminelt skal politiet varsles. Ansatte bør ikke ta selv ta seg inn til hendelsesstedet, men vente til politiet kommer på stedet.

Det anbefales videre at pumper og annet utstyr som vurderes som viktig for vannforsyningen er tilkoblet nødstrømsaggregat, slik at vannforsyningen fortsatt kan fungere selv om strømtilførselen skulle falle ut eller bli sabotert.

Eksempel på grunnvannsbrønner som bør sikres.

Grunnsikring	**Barrierer** *Skallsikring:* ▪ Dører bør være sikkerhetsgodkjente etter ENV 1627 klasse 3 med FG-godkjente låser alternativt kan det monteres et tilsvarende sikkerhetsgodkjent rullegitter foran en svakere dør. ▪ Om mulig kle/støp igjen vinduer og sikre dem tilsvarende vegg. Alternativt kan det monteres sikkerhetsgodkjent gitter eller rullegitter foran vinduer med tilsvarende styrkegrad som dør. ▪ Det bør vurderes om det skal etableres kompenserende sikringstiltak for å veie opp for en eventuell svak skallsikring som er svært kostbar å forsterke. Dette kan for eksempel være et perimetergjerdet med deteksjonstiltak. **Deteksjon og verifikasjon** *Elektronisk sikring:* ▪ Etablere innbruddsalarm på innsiden av bygget/installasjonen med utvendig og innvendig sirene som overføres til alarmmottak/driftssentral. Innbruddsalarmen bør minimum bestå av magnetkontakt på dør og passive infrarøde detektorer. ▪ Det bør etableres lyskastere med bevegelsessensor rundt bygget/installasjonen. **Reaksjon** *Vakt- og reaksjonsstyrke og varslingssystemer* ▪ Utarbeide rutiner for at vekter og/eller ansatt overvåker og responderer på utløste alarmer ▪ Etablere beredskapsplaner og varslingsrutiner for verifiserte alarmer (objektinstruks) ▪ Ved en verifisert (reell) alarm varsles politiet. ▪ Varsling av abonnenter og lokalbefolkningen iht. beredskapsplan og etter dialog med helse- og tilsynsmyndigheter, dersom det er usikkerhet rundt om drikkevannet er forurenset/forgiftet. **Gjenoppretting** *Redundans på støttesystemer* ▪ I forbindelse med beredskapsplanleggingen bør det vurderes om pumper og annet utstyr som viktig for vannforsyningen skal eget nødstrømsaggregat eller mulighet for tilkobling til mobilt aggregat.
Tilleggssikring	**Barrierer** *Perimeter og skallsikring:* ▪ Det bør etableres et perimetergjerdet (minimum 2 meter) rundt bygget/installasjonen. ▪ Dersom trebygget har svak skallsikring bør vegger/tak forsterkes innvendig med 3 mm stålplate og 16 mm kryssfiner. Vinduer bør ha tilsvarende styrkegrad som vegger. **Deteksjon og verifikasjon** *Elektronisk sikring:* ▪ Etablere TV-overvåkning utenfor i bygningen for å verifisere alarmer. Kamerabildet overføres til alarmmottak/driftssentral. Dersom det ikke er mulig med kameraoverføring må det etableres en rutine for at vekter og/eller en ansatt kan responderer på utløste alarmer. I et slikt tilfelle bør vurderes om man også skal settes opp et viltkamera slik at hendelsen blir dokumentert. ▪ Nøkkelbasert låssystem erstattes med et elektronisk adgangskontrollsystem

Figur 14: *Beskrivelse av grunnsikring og tilleggssikring for bygg eller annen installasjon for grunnvannskilde og råvannsinntak.*

6.2.3. Vannbehandlingsanlegg

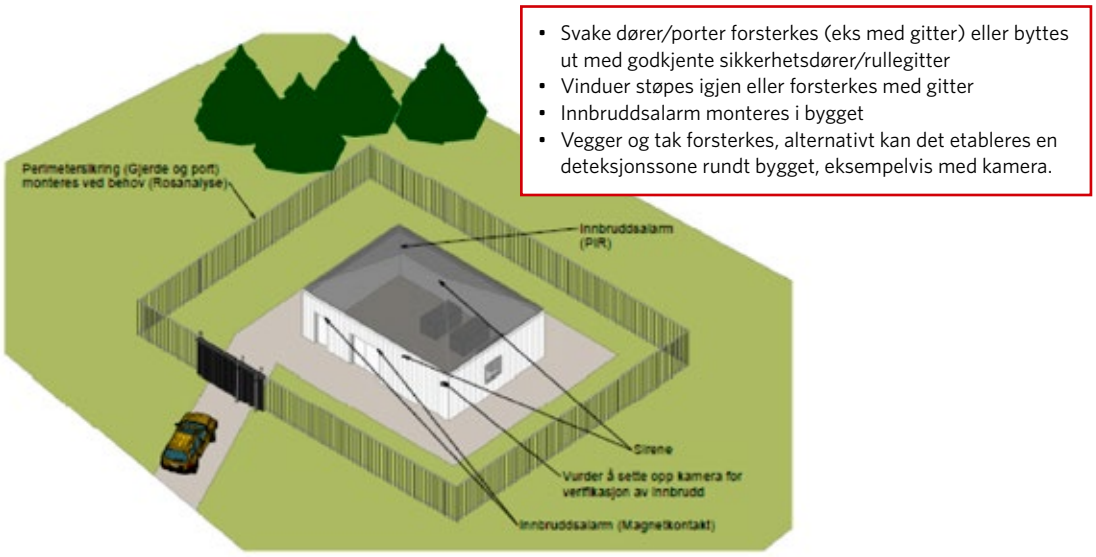
Det finnes i dag en rekke ulike vannbehandlingsanlegg i Norge. Anleggene kan bestå av et eller flere bygg. Flere anlegg har også blitt lagt inn i fjell. I tillegg til at vannbehandlingsprosessen finner sted i vannbehandlingsanleggene huser disse bygningene gjerne også en rekke andre funksjoner, blant annet administrative Den lokale vannforsyningens driftssentral, servere og kommunikasjonssystemer er ofte også lokalisert i disse anleggene eller i nær tilknytning til dem. Med sine mange funksjoner utgjør vannbehandlingsanlegget selve «hjerte» i vannforsyningssystemet og er derfor blant delene av vannforsyningen som det er viktigst å sikre.

For å forsterke skallsikringen kan man ta i bruk stålplater og kryssfiner samt bytte ut eksisterende dører med sikkerhetsdører med FG-godkjente dører. Det anbefale videre at vinduer som ikke har en nødvendig funksjon støpes eller kles igjen og sikres tilsvarende som vegg. Alternativt kan det monteres sikkerhetsgodkjente gitter eller rullegitter. For at et eventuelt angrep skal detekteres og verifiserer bør også bygninger og deler av bygninger som huser viktige funksjoner utstyres med innbruddsalarm og TV-overvåkning. Kamerabildet overføres til alarmmottak/driftssentral.

Dersom en forsterkning av den fysiske skallsikringen blir for kostbar til å gjennomføre kan et kompenserende sikringstiltak være å etablere et perimetergjerdet rundt eiendommen. Perimetergjerdet og/eller uteområdet bør da være utstyr med en form for deteksjon- og verifikasjonstiltak slik at man kan få en tidlig deteksjon av inntrengningen og verifikasjon av inntrengningen og raskt kan iverksette riktige reaksjonstiltak. Dette kan være i form av et termisk- og optisk TV-overvåkningskamera.

Felles for de fleste norske vannbehandlingsanlegg er at de i liten grad har blitt delt inn i adskilte sikringssoner innvendig. Dersom man først kommer på innsiden av anlegget vil man i mange tilfeller få direkte tilgang drikkevannstrømmen på ulike stadier i renseprosessen, så vel som drikkevannsbassenger med åpent vannspeil. Det er derfor svært viktig å etablere og opprettholde et strengt sikkerhetsregime for adgang til anleggene. Det anbefales at det etableres adgangskontroll på alle innganger inn til anlegget og inn til viktige funksjonene inne i anlegget. Videre anbefales det at vannverkene gjennomfører sikkerhetssamtale med personer som skal gis selvstendig adgang. Dersom vedkommende kun har behov for adgang for en kort periode bør personen følges av en fast ansatt. Det er også nødvendig at det etableres en god sikkerhetskultur i organisasjonen. For spesielt viktige funksjoner i anlegget, for eksempel driftssentral, serverrom og arealer med direkte tilgang til vannspeil, anbefales at det etableres egne sikringssoner. Dette kan gjøres ved å etablere en skallsikring rundt sonene og å ha et separat låssystem for disse sonene. Erfaringsvis er nøkler vanskelig å ha kontroll på så det bør derfor vurderes å montere adgangskontrollanlegg for å regulere adgangen til sonene. Sikringssonene vil utgjøre en sikring i dybden og medfører en økt inntrengningstid.

Videre bør det etableres redundans på sentrale støttesystemer som vannbehandlingsanlegget er avhengig av. Hvilke systemer dette er bør fremkomme i ROS-analysen. Dette kan gjøres for eksempel ved å etablere UPS og nødstrømsaggregatet eller ved å etablere flere kommunikasjonssystemer (som fiber, GPRS og radio) inn til anlegget.



Figur 15: *Prinsippskisse sikring av eksisterende bygg.*

Grunnsikring	**Barrierer** *Perimetersikring:* ▪ Det bør vurderes om det skal etableres kompenserende sikringstiltak for å veie opp for en eventuell svak skallsikring. Dette kan for eksempel være et perimetergjerdet (minimum 2 meter) rundt eiendommen. Kombinert med deteksjons- og verifikasjonstiltak. (Se elektronisk sikring). *Skallsikring:* ▪ Etablere sikkerhetsgodkjente dører etter ENV 1627 klasse 3 med FG-godkjente låser eller tilsvarende rullegitter. ▪ Om mulig kle igjen vinduer/støp igjen og sikre dem tilsvarende vegg. Alternativt kan det monteres faste gitter eller sikkerhetsgodkjent rullegitter foran vinduer med tilsvarende styrkegrad som dør. ▪ Det bør vurderes om den eksiterende bygningsmassen (tak og vegger) også skal forsterkes. Dette kan gjøres ved at vegger og tak forsterkes innvendig med 3 mm stålplate og 16 mm kryssfiner. **Deteksjon og verifikasjon** *Elektronisk sikring:* ▪ Perimetergjerdet og/eller uteområdet utstyres med deteksjon- og verifikasjontiltak for eksempel termiske og optiske TV-overvåkningskamera. ▪ Det bør etableres lyskastere med bevegelsessensor rundt bygget/installasjonen. ▪ Etablere innbruddsalarm på innsiden av bygget med utvendig og innvendig sirene og overføring til alarmmottak/driftssentral. Innbruddsalarmen bør minimum bestå av magnetkontakter på dører og passive infrarøde detektorer. ▪ Etablere adgangskontroll på alle innganger inn til vannbehandlingsanlegget samt inn til sentrale funksjoner inne anlegget. **Reaksjon** *Vakt- og reaksjonsstyrke og varslingssystemer* ▪ Utarbeide rutiner for at vekter og/eller ansatt overvåker og responderer på utløste alarmer. ▪ Etablere beredskapsplaner og varslingsrutiner for verifiserte alarmer. ▪ Ved en verifisert (reell) alarm varsles politiet. ▪ Varsling av abonnenter og lokalbefolkningen iht. beredskapsplan og etter dialog med helse- og tilsynsmyndigheter, dersom det er usikkerhet rundt om drikkevannet er forurenset/forgiftet. **Gjenoppretting** *Støttesystemer* ▪ Etablere redundans på viktige støttesystemer.
Tilleggssikring	**Barrierer** *Perimetersikring:* ▪ Etablere perimetergjerdet (minimum 2 meter) rundt anlegget. *Skallsikring:* ▪ Dersom trebygget har svak skallsikring bør vegger/tak forsterkes innvendig med 3 mm stålplate og 16 mm kryssfiner. Vinduer bør ha tilsvarende styrkegrad som vegger. **Deteksjon og verifikasjon** *Elektronisk sikring:* ▪ Monter deteksjon- og verifikasjonstiltak på innsiden av perimetergjerde for eksempel med termiske og optiske kamera for å sikre en rask reaksjon.

Figur 16: *Beskrivelse av grunnsikring og tilleggssikring for vannbehandlingsanlegg.*

6.2.4. Ledningsnett og kummer

Ledningsnettet er blant de delene av vannforsyningen som det er mest utfordrende å sikre. Dette skyldes i all hovedsak ledningsnettets omfang og tilgjengelighet. Ut fra hensynet til driftssikkerhet er ledningsnettet ofte bygget med tosidig forsyning, eller andre muligheter for å legge inn omreguleringer ved utfall. Dette er også gunstig sett ut fra et sikringsståsted. Videre er det gjerne overvåket via et fjernkontrollsystem, og uregelmessigheter i trykk/mengde blir raskt detektert av driftsorganisasjonen. Og erfaringsmessig får kommunen/vannverkseier raskt varsel fra publikum dersom det oppstår avbrudd i forsyningen. Mulighetene for å påføre mange mennesker skade som følge av bortfall av vann er således begrenset, dersom angriperen ikke har kapasitet til å utføre svært mange sabotasjehandlinger

samtidig. Samtidig har de fleste vannverkseiere god beredskap for raskt å reparere avbrudd i ledningsnettet. Man kan i et ekstremt tilfelle tenke seg at en virkelig ondsinnet aktør kan tilføre ledningsnettet agens som forgifter eller forringer drikkevannet. Imidlertid vil målrettede angrep av denne karakter kreve god kunnskap om vannforsyningssystemet oppbygging, strømningsretninger etc. Dette tilsier at vannverkseierne bør ha et bevisst forhold til hvordan ledningskartverket sikres.

Med utgangspunkt i en ROS-analysen kan man vurderer om det er utvalgte deler som skal sikres særskilt. Dette kan for eksempel være deler av ledningsnettet som leder inn til andre kritiske samfunnsfunksjoner som et sykehus, en forsvarsinstallasjon eller et andre offentlige eller kommunale bygg. Vannverkene bør her gå i dialog med den aktuelle virksomheten for å avklare om de har særksilte sikringsbehov og evt. diskutere gjennomføring av konkrete sikringstiltak.

For særlig utsatte deler av ledningsnettet bør det vurderes om kummer skal sikres særskilt for eksempel med låsbart underlokk og alarmsensor. På denne måten kan en eventuell inntrengning detekteres og man kan iverksette reaksjonstiltak. Et viktig reaksjonstiltak vil være å etablere rutiner for å varsle lokalbefolkningen dersom det er usikkerhet rundt hvorvidt vannet i ledningsnettet kan være forgiftet/forurenset.

Grunnsikring	**Barrierer** *Skallsikring:* ▪ Ledningsnettet er normalt nedgravd. Særskilte kuminstallasjoner kan vurderes utstyrt med låsbare kumlokk. **Deteksjon og verifikasjon** *Elektronisk sikring:* ▪ Vurder å monter alarmsensor i kummer i særlig utsatte deler av ledningsnettet eller inn til samfunnskritiske abonnenter. **Reaksjon** *Vakt- og reaksjonsstyrke og varslingssystemer* ▪ Etablere beredskapsplaner og varslingsrutiner for verifiserte hendelser. ▪ Ved en verifisert (reell) hendelse varsles politiet. ▪ Varsling av abonnenter og lokalbefolkningen iht. beredskapsplan og etter dialog med helse- og tilsynsmyndigheter, dersom det er usikkerhet rundt om drikkevannet er forurenset/forgiftet. **Gjenopprettelse** *Reparasjon:* ▪ Etablere beredskap til å reparere eventuelle ledningsbrudd, gjennomføre omreguleringer/legge inn reservevann.
Tilleggssikring	**Barrierer** *Skallsikring:* ▪ Øke omfanget av skallsikring (låsbare kumlokk) på viktige kummer. **Deteksjon og verifikasjon** *Elektronisk sikring:* ▪ Kummer i særlig utsatte deler av ledningsnettet eller inn til samfunnskritiske abonnenter som utstyres med alarmsensor (eks magnetkontakt). **Reaksjon** *Vakt- og reaksjonsstyrke og varslingssystemer* ▪ Utarbeide rutiner for at vekter og/eller ansatt overvåker og responderer på utløste alarmer.

Figur 17: *Beskrivelse av grunnsikring og tilleggssikring for ledningsnett og kummer.*

6.2.5. Pumpestasjoner

Større pumpestasjoner består gjerne av et bygg med inntaksrør, fordelingsrør og pumper. Bygget kan være utført i både betong og murverk, men de fleste av de eksisterende byggene er utført i trevirke og kun utstyrt med enkle dører og vinduer uten spesiell sikring. Mindre pumpestasjoner er gjerne lagt i kum eller liknende.

Det anbefales derfor at større pumpestasjoner sikres på samme måte som bygg eller annen installasjon for grunnvannskilde og råvannsinntak beskrevet i delkapittel *6.2.2 Bygg eller annen installasjon for grunnvannskilde og råvannsinntak,* mens mindre pumpestasjoner sikres på samme måte som kummer beskrevet i delkapittel *6.2.4 Ledningsnett og kummer*.

6.2.6. Høydebasseng

Sammen med vannbehandlingsanleggene er høydebassengene blant delene av vannforsyningen som det er viktigst å sikre. Dette følger blant annet av at høydebassengene er plassert etter vannbehandlingsanlegget i forsyningsprosessen, og vannet derfor ikke gjennomgår flere hygieniske barrierer før det distribueres ut til abonnentene. I tillegg er høydebassengene ofte plassert i et stykke unna boligbebyggelse og det er således få som vil kunne observere om det er mistenkelig aktivitet rundt bassengene.

Det finnes i dag en rekke ulike typer høydebasseng – både i design og utførelse. Norske høydebasseng kan være plassert i fjellanlegg, nedgravd eller bestå av et overflatebygg. For de av høydebassengene som er plassert i fjell eller nedgrav ligger forholdene til rette for å kunne etablere en god skallsikring. Dette følger av at det som regel er brukt armert betong i vegger i tunnelåpninger og i hele konstruksjonen for nedgravde basseng. For nedgravde basseng er det imidlertid viktig å huske på at taket av bassenget vil være lett tilgjengelig og at det derfor er svært viktig å sikre både inspeksjonsluke og lufterør godt. I dette delkapittelet vil imidlertid hovedvekten legges på overflatebygg, da dette er typen høydebasseng det er flest av og hvor sikringsutfordringen er størst.

De fleste overflatebygg er utført i betong eller teglstein som har moderat til høy styrkegrad. Det finnes imidlertid også bassenger med tynne vegger som er utført i glassfiber, stål eller liknende. Disse byggene har en lavere styrkegrad og det bør derfor vurderes om disse skal forsterkes. Erfaringsmessig kan dette imidlertid være svært kostbart. Dersom forsterkning av den eksisterende skallsikring ikke er mulig å gjennomføre eller det vurderes som lite hensiktsmessig anbefales at det etableres kompenserende tiltak. Et slikt tiltak kan være at det etableres et perimetergjerdet rundt høydebassenget. På innsiden av perimetergjerdet bør settes opp termisk- og optisk kamera slik at man får en tidlig deteksjon og verifikasjon av en eventuell inntrengning. Et annet kompenserende tiltak som anbefales er at det etableres mulighet for å åpne/lukke ventilene fra driftssentralen. Bassenget vil da kunne stenges av fra ledningsnettet/distribusjonssystemet midlertidig dersom det er usikkert om det har blitt forurenset/forgiftet.

Alle høydebasseng har en nedstigningsluke og et eller flere rør for lufting av vannkammeret. Disse befinner seg som regel på taket av høydebassenget og kan utnyttes i et angrep mot vannmagasinet. Både nedstigningsluke og luftingventiler må derfor sikres. I tillegg bør eventuell utvendig stige opp til taket av bassenget fjernes eller sikres for å vanskeligjøre tilgang til taket. Det finne i dag en rekke gode løsninger for å sikre disse komponentene. Der risikoen vurderes som høy i ROS-analysen anbefales det å bygge et trappetårn i tilknytning til høydebassenget. Trappetårnet bør omslutte både stige, nedstigingsluke og lufting. For nedgravde bassenger anbefales at det bygges et overbygg i betong over bassenget. For alle løsninger anbefales det at konstruksjonen utstyres med sikkerhetsdør med alarmsensorer minimum i form av en magnetkontakt på dører/luker og innvendig bevegelsesdetektor (PIR) slik at en eventuell inntrengning detekteres tidlig.

Alle lufterør og eventuelle andre rør inn/ut til vannkammeret som ikke er plassert i et teknisk rom må sikres. Dette for å hindre at uvedkommende kan føre gjenstander eller trusselstoffer inn i vannkammeret. Det bør her etableres to sikkerhetsbarrierer. Den første kan være et gitter som etableres foran ventilen, mens den andre barrieren kan være en solid kasse av stål som monteres og boltes fast over ventilen(e). Denne kassen må ha åpninger for lufting og/eller drenering som også sikres med gitter. For å hindre at noen prøver å tre en slange eller lignende gjennom begge sikkerhetsbarrierer må disse ikke plasseres rett ovenfor hverandre. Spesialdesignet luftventiler som hindrer at det føres trusselstoffer inn via ventilen finnes også. Videre bør nedstigningsluken byttes ut med en solid inspeksjonsluke i stål og sikres med en kraftig FG-godkjent hengelås. Hengelåsen bør utstyres med en stålkappe over for å hindre at bøylen enkelt kan kuttes.

Eksempler på ulike sikringsløsninger for høydebasseng.

Figur 18 *viser overflatebasseng utført i betong med påbygget trappetårn og perimetergjerde. (foto Ancistrus AS).*

Figur 19 *viser overflatebasseng utført i betong med heldekkende sylinder rundt stigen og hus på taket. (foto Ancistrus AS).*

Figur 20 *viser nedgravd høydebasseng med overbygg i betong. (foto Ancistrus AS).*

Figur 21 *viser nedgravd høydebasseng med overbygd hus i trevirke. (foto Forsvarsbygg)*

Grunnsikring	**Barrierer** *Perimetersikring:* ▪ For høydebasseng utført i materialer med lav styrkegrad etableres et perimetergjerdet (minimum 2 meter) rundt bassengkonstruksjonen. Kombinert med deteksjons- og verifikasjontiltak. (Se elektronisk sikring) *Skallsikring:* ▪ Nedstigningsluke byttes ut med en solid luke i stål som sikres med kraftig hengelås og ståldeksel. ▪ Frittstående ventiler på vegg eller tak må sikres mot innføring av gjenstander eller væske (se beskrivelse i avsnittet ovenfor). ▪ Utvendig stige opp til taket av bassenget bør fjernes eller sikres for å vanskeliggjøre tilgang til taket. **Deteksjon og verifikasjon** *Elektronisk sikring:* ▪ På innsiden av perimetergjerdet bør det etableres deteksjon- og verifikasjonstiltak som for eksempel termiske og optiske kamera for å sikre en rask reaksjon. ▪ Etablere innbruddsalarm på innsiden av inspeksjonsluke (magnetkontakt). **Reaksjon** *Vakt- og reaksjonsstyrke og varslingssystemer* ▪ Utarbeide rutiner for at vekter og/eller ansatt overvåker og responderer på utløste alarmer. ▪ Etablere beredskapsplaner og varslingsrutiner verifiserte alarmer. ▪ Ved en verifisert (reell) alarm varsles politiet. ▪ Varsling av abonnenter og lokalbefolkningen iht. beredskapsplan og etter dialog med helse- og tilsynsmyndigheter, dersom det er usikkerhet rundt om drikkevannet er forurenset/forgiftet. ▪ Etablere motoriserte ventiler som gir mulighet for å åpne/lukke ventilene fra driftssentralen.
Tilleggssikring	**Barrierer** *Perimetersikring:* ▪ Etableres et perimetergjerdet (minimum 2 meter) rundt bassengkonstruksjonen. *Skallsikring:* ▪ Det bør vurderes om det skal etableres et trappetårn, et overbygg eller andre løsninger for ytterligere sikring av nedstigningsluke og lufting. Det anbefales at dette bygges i 15 cm betong. ▪ Trappetårnet/overbygget utstyres med sikkerhetsdør med FG-godkjent lås og utføres uten vinduer. **Deteksjon og verifikasjon** *Elektronisk sikring:* ▪ Trappetårnet/overbygget bør utstyres med magnetkontakt eller passiv infrarød detektor innvendig med overføring til alarmmottak/driftssentral. ▪ Etabler utvendig sirene.

Figur 22: *Beskrivelse av grunnsikring og tilleggssikring for høydebasseng.*

6.2.7. Nybygg

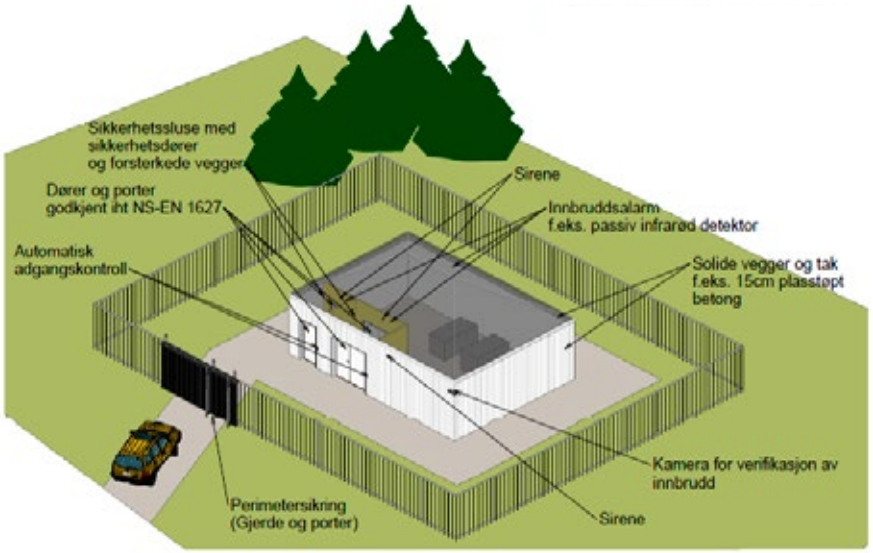
Ved bygging av nye større bygg tilknyttet distribusjonssystemet og vannbehandlingsanlegg er det avgjørende at sikringsbehovene kartlegges tidlig i byggeprosjektet slik at relevante sikringstiltak blir tatt med i byggebeskrivelsen. Også dette bør gjøres med utgangspunkt i en oppdatert ROS-analyse.

Levetiden på et bygg er minst 40 år. For at man også skal kunne møte eventuelle nye trusselscenarier i fremtiden anbefales at man velger en robust og kraftig konstruksjon når man skal planlegge og bygger nye samfunnskritiske bygg og anlegg. For at bygget også skal kunne ha en relativt god fysisk sikring mot inntrengning også i framtiden anbefales at alle bygg utføres i armert betong og at det benyttes sikkerhetsdører og –porter, godkjent etter ENV 1627 klasse 3 med to FG-godkjente låser. På innsiden av dør bør det også vurderes å etablere en sikkerhetssluse i betong slik at man passerer to sikkerhetsbarrierer før man er inne i bygget. Dette vil gi god sikring i dybden og en økt inntrengningstid. Vinduer kan være et svakt punkt i skallsikringen. Dersom det ikke er nødvendig anbefales derfor at det ikke planlegges med vinduer i bygget. Alternativt må vinduer sikres med sikkerhetsgodkjent gitter, godkjent etter ENV 1627 i samme klasse som dør/porter.

Videre anbefales at det etableres et perimeter rundt bygget bestående av minimum et 2 meter høyt solid

flettverksgjerde. På gjerdet bør det monteres skilt med advarsler og varsel om at området er kameraovervåket. For å verifisere alarmer på en effektiv måte bør det settes opp et TV-overvåkningskamera med IR-lys på mast eller vegg. Det bør også etableres flombelysning med bevegelsessensor på alle byggets sider. Lyset må ikke blende kameraene.

For å kunne styre adgangen til bygget på en effektiv og god måte bør det vurderes å installere adgangskontrollsystem på dører og porter. Bygget bør videre utstyres med innbruddsalarm med minimum magnetkontaker i dør/porter/luker og passiv infrarøde detektorer i sikkerhetssluse og inne i bygget. For spesielt viktige områder i nye vannbehandlingsanlegg bør det også etableres adgangskontroll, innbruddsalarm og TV-overvåkning. Alarmer og kamerabilder overføres til driftssentral eller alarmmottak. For å skremme vekk inntrengere eller varsle folk i nærområdet anbefales at det etableres en sirene i både sluse og på utsiden av bygningen. Sirenen bør har et lydnivå på ca. 120 dB for å gjøre det ubehagelig å oppholde seg i slusen eller inne i bygget. Et annet salternativ er å etablere et tåkeanlegg i slusen. Dette vil gjøre at inntrenger mister oversikt og orienteringsevne. Andre tiltak som kan vurderes er opptak av lyd fra innbruddsforsøket og talevarsling. Dersom inntrengerne får beskjed over høyttaler at de er oppdaget og at politiet er på vei kan dette føre til at de avbryter innbruddsforsøket. Beskjedene bør gis på både norsk og engelsk.



Figur 23: Prinsippskisse som viser sikring av nybygg

Grunnsikring nybygg	**Barrierer** *Perimetersikring:* ▪ For større bygg eller samlinger av bygg bør det etableres et perimetergjerdet (minimum 2 meter) med en låsbar kjøreport. *Skallsikring:* ▪ Bygget bør utføres i minimum 15 cm armert betong med sikkerhetsdør/port, godkjent etter ENV 1627 klasse 3 med to FG godkjente låser. ▪ Om mulig bør vinduer unngås. Alternativt må vinduer sikres med sikkerhetsgodkjent gitter, godkjent etter ENV 1627 i samme klasse som dør/porter. ▪ Ved innganger til bygget bør det etableres en sikkerhetssluse for å få en ekstra sikkerhetsbarriere i inngangspartiet. **Deteksjon og verifikasjon** *Elektronisk sikring:* ▪ Det bør etableres innbruddsalarm inne i bygget med minimum magnetkontakter på dører/porter og passiv infrarød detektorer med overføring til alarmmottak/driftssentral. ▪ Det bør etableres sirene både på innsiden og utsiden av bygningen. ▪ Det bør etableres TV-overvåkningskamera (optisk) med IR-lys for verifikasjon av alarm på utsiden av bygningen. ▪ Det bør etableres flomlys med bevegelsessensor på alle sider av byggets utside. ▪ Ulike sikringstiltak som tåkesikring, opptak av lyd og høyttaler for å advare inntrengerne bør vurderes. **Reaksjon** *Vakt- og reaksjonsstyrke og varslingssystemer* ▪ Ved etablering av nybygg må det kontrolleres om alarmmottaket/driftssentralen kan håndtere og verifisere alarmer og at det er etablert rutiner for å varsle politi, ansatte, eiere og abonnenter.

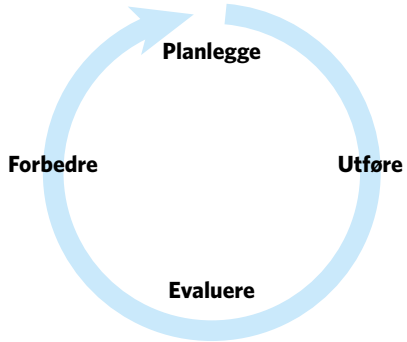
Figur 24: *Beskrivelse av grunnsikring for nybygg.*

6.2.8. Hvordan oppnå en tilstrekkelig sikring? (sjekkliste)

Den norske vannforsyningen er definert som en samfunnskritisk funksjon fordi tilgang på vann er en grunnleggende fysiologisk forutsetning for alt liv og viktig av hygieniske samt sanitære årsaker. Svikt i drikkevannsforsyningen vil også kunne få konsekvenser for samfunnets evne til å ivareta en rekke andre kritiske funksjoner. [57)]

I henhold til drikkevannsforskriften § 10 skal vannverkseieren sikre at vannbehandlingsanlegget og alle relevante deler av distribusjonssystemet er tilstrekkelig fysisk sikret. Hva som anses som tilstrekkelig sikret og hvilke deler av distribusjonssystemet som er relevante å sikre må fremkomme av en ROS-analyse. Alle norske vannforsyningssystemer, uavhengig av størrelse, beliggenhet og kritiske abonnenter, bør imidlertid ha en god grunnsikring mot tilsiktede uønskede handlinger som kan ramme vannforsyningen. Der ROS-analysen viser at et vannforsyningssystem er særlig utsatt, eller at skadeomfanget ved en slik hendelser er særlig høyt, bør det imidlertid etableres en tilleggssikring. En beskrivelse av et forslag til en slik grunnsikring og tilleggssikring er gitt i kapitlene over.

For å tilfredsstille drikkevannsforskriftens krav er det avgjørende med en helhetlig tilnærming til sikring. Dette er en sikring som ikke bare omfatter fysiske sikringstiltak, men også elektronisk sikring, administrative og organisatoriske sikringstiltak. Tiltakene bør bestå av en kombinasjon av barrierer, deteksjon, verifikasjon og reaksjon som er tilpasset det enkelte vannforsyningssystemet. I tillegg må man jobbe systematisk med å planlegge, evaluere og forbedre sikringen og beredskapsplanverket, for eksempel gjennom øvelser og sikkerhetsrevisjoner.



Figur 25: *Eksempel på en planleggingssyklus for beredskapsarbeid*

57) DBS, Samfunnskritiske funksjoner – Hvilke funksjonsevne må samfunnet opprettholde over enhver tid? 2016, 79-81

Sjekkliste for å oppnå en tilstrekkelig sikring av vannforsyningen mot tilsiktede hendelser

Under følger en sjekkliste over generelle sikringstiltak som det enkelte vannforsyningssystem bør ha gjennomført for å oppnå en tilstrekkelig sikring av vannforsyningen. Listen oppsummerer kort de viktigste anbefalingene gitt i denne veilederen.

	Oppdaterte risikoanalyser Alle vannverk må ha oppdatere risikoanalyser som omfatter alle relevante deler av vannforsyningen og som omfatter relevante security scenario. Risikoanalysen bør oppdateres ved jevne mellomrom eller dersom noen av innsatsfaktorene (verdi, trussel, sårbarhet) endrer seg.
	Bakgrunnssjekk av nyansatte og oppfølging av ansatte Alle vannverk bør etablere rutiner for bakgrunnssjekk av nyansatte. En bakgrunnssjekk kan avdekke alt fra uregelmessigheter knyttet til CV, utdannelse, kompetanse og identitet til historie med ytterliggående ytringer, brudd på straffeloven, omdømmesaker, konflikter og rusproblematikk. Den beste bakgrunnssjekken får man ved å sikkerhetsklare ansatte, men per dags dato er det få vannverk som har mulighet til dette. Alle vannverk bør derfor lage en prosedyre for hvordan man kan gjennomføre egen bakgrunnssjekk. Det bør også etableres rutiner for sikkerhetsmessig oppfølging av ansatte med årlige samtaler om forhold som kan påvirke den ansattes dømmekraft og vurderingsevne (f.eks dårlig økonomi, kriminell adferd, kontakter med andre stater og dårlig psykisk helse). For mer informasjon om dette tema se Veileder for sikkerhet ved ansettelsesforhold, utarbeidet av Politiet, Nasjonal sikkerhetsmyndighet, Næringslivets sikkerhetsråd og Politiets sikkerhetstjeneste.
	Etablere god sikkerhetskultur og rutiner for sikkerhetsopplæring Alle vannverk må etablere en god sikkerhetskultur og harutiner for grunnleggende sikkerhetsopplæring av ansatte og andre som gis adgang til hele eller deler av vannforsyningen. Det er et lederansvar å legge til rette for en god sikkerhetskultur i virksomheten.
	Retningslinjer for informasjonssikkerhet Alle vannverk bør ha etablert retningslinjer for informasjonssikkerhet. Disse retningslinjene bør gir anvisninger for sikker lagring, deling og håndtering av sensitiv informasjon (bør etableres etter «need-to-know-prinsippet»). Sensitiv informasjon bør merkes med Fortrolig, Meget Fortrolig (Beskyttelsesinstruksen) eller Unntatt offentligheten.
	Fysiske barrierer og andre forsinkende/avskrekkende tiltak Alle vannverk skal ha etablert ulike fysiske barrierer og andre tiltak som skal søke å avskrekke, forsinke eller stoppe en inntrenger. Eksempel på slike tiltak er å etablere en god skallsikring bygg, godkjente sikkerhetsdører, sikkerhetsluse, flomlys, skilting, kameraovervåkning, sirene, lydopptak og talevarsling.
	Kontroll på adgangen til viktige deler av vannforsyningen Alle vannverk bør ha et system som styrer og loggfører hvem som gis adgang til de viktigste delene av vannforsyningen. Kun de som har tjenstlig behov skal gis adgang. Adgangslistene bør derfor gjennomgås jevnlig og personer som ikke har lenger har behov for adgang må fjernes fra listen umiddelbart. Ideelt sett bør det etableres et automatisk adgangskontrollsystem (AAK), men for enkle anlegg kan man ha et nøkkelsystem forutsatt at det etableres et system for å sikre at nøkler ikke kommer på avveie.

	Systemer for deteksjon Alle vannverk må ha etablert et innbruddsalarmsystem som skal varsle når noen tar seg ulovlig inn i sentrale deler av vannforsyningssystemet (råvanninntak, pumpehus, høydebasseng, vannbehandlingsanlegg og driftskontrollanlegg). Disse alarmene sendes til driftssentralen eller til en godkjent alarmstasjon.
	Systemer for verifikasjon Alle vannverk må ha etablert et system for å verifisere alarmer fra alarmsystemet. Verifisering av alarmen kan skje ved at egne ansatte eller et vekterselskap rykker ut eller helst ved bruk av TV-overvåkning (TVO).
	Systemer for reaksjon Alle vannverk må ha en reaksjonsplan for å varsle egne ansatte, politi, abbonnenter, kommuner, myndigheter o.l. ved en eventuell uønsket hendelse. Vannverkene bør øve på innsats fra politiet ved en sikkerhetshendelse.
	Planer og rutiner for gjenoppretting og skadereduserende tiltak Alle vannverk må ha planer og etablerte rutiner for gjenoppretting og skadereduserende tiltak ved en eventuell uønsket tilsiktet hendelser. Disse bør være øvet på forhånd.
	Beredskapsplan og beredskapsøvelser Alle vannverk må ha en plan for å kunne forsterke grunnsikringen ved en økt trussel. Disse planene bør være øvet på forhånd. Det bør etableres en egen oversikt over planlagte og gjennomførte øvelser.
	Registrere alle avvik, sikkerhetsbrudd og sikkerhetstruende hendelser (eks innbrudd, hærverk) Det vil være viktig grunnlagsdata for oppdatering av ROS-analysen og for å vurdere behov for ekstra sikring og opplæring.
	Datasikkerhet Alle vannverk må sikre sine data- og driftssystemer mot cybertrusler (beskrives ikke i denne rapporten).

Referanser

Busmundrud m.fl., *Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger*, FFI-rapport 2015/00923 2015

Bartnes, Jørgen m.fl., *Sårbarhet i vannforsyningen*, Scandpower Risk Management/FFI/Auqateam/Cowi AS, 2003

Brombach, Harald, *«Falske GPS-signaler narret navigasjonsutstyret til flere titalls skip»* i Teknisk ukeblad, 11.08.17. Tilgjengelig på: https://www.nrk.no/finnmark/stoy-fra-russland-slo-ut-gps-signaler-for-norske-fly-1.13720305

Claudia Copeland, *«Terrorisme and Security Issues Faceing the Water Infrastructure Sector»* i Congressional Research Service, 2010

CPNI, CPNI Insider Data Collection Study: *Report of Main Findings*, 2013.

DBS, *Samfunnskritiske funksjoner – Hvilke funksjonsevne må samfunnet opprettholde over enhver tid?*, 2016

DSB, *Veileder til helhetlig risiko- og sårbarhetsanalyse i kommunen*, 2014

Etterretningstjenesten, Fokus 2017 – *Etteretningstenesta si vurdering av aktuelle tryggingsutfordringar*, 2017

Finsveen, Jesper Nordahl, *«Tror fremmede makter kan stå bak maktsabotasje i Sverige. Kan være en stresstest ifølge politiet»* i Dagbladet, 17.05.16. Tilgjengelig på: https://www.dagbladet.no/nyheter/tror-fremmede-makter-star-bak-mastsabotasje-i-sverige-kan-vaere-en-stresstest-ifolge-politiet/60382242

Forsvarsbygg, Sikringshåndboka, 2016

Horn, Knut-Sverre, *«Støy fra Russland slo ut GPS-signaler for norske fly»* på NRK.no, 05.10.2017. Tilgjengelig på: https://www.nrk.no/finnmark/stoy-fra-russland-slo-ut-gps-signaler-for-norske-fly-1.13720305

Johnsrud, Ingar m.fl., *«Kunne ha stoppet vanntilførselen med mobilen»*, 09.09.11, https://www.vg.no/nyheter/innenriks/terrortrusselen-mot-norge/kunne-stoppet-vanntilfoerselen-med-mobilen/a/10098352/

Jore, Sissel, *«Safety and Security – is there a need for an integrated approach?»* i Risk, Reliability and Safety: Innovating Theory and Practice : Proceedings of ESREL 2016 (Glasgow, Scotland, 25 – 29 September 2016). CRC Press. ISBN 9781138029972

Jore, Sissel og Egeli, *«Risk management methodology for protecting against malicous acts – Are probabilites adequate means for describing terrorisme and other security risks?»* fra European Safety and Reliability Conference (ESREL), 2015, Zurich Switzerland.

Kirkebøen, Stein Erik, *«1972: Bonde helt gift i Oslos drikkevann»* i Aftenposten, 16.07.2015. Tilgjengelig på: https://www.aftenposten.no/osloby/i/5vVX/1972-Bonde-helte-gift-i-Oslos-drikkevann

Kirkebøen, Stein Erik, *«Hemmelig rapport fra 2013 med kraftig kritikk av Oslos drikkevannssikring»*, 17.06.2015, https://www.aftenposten.no/osloby/i/q8no/Hemmelig-rapport-fra-2013-med-kraftig-kritikk-av-Oslos-drikkevanns-sikring

Kirkebøen, Stein Erik, Aslabeehg: *– Byrådet har ikke gjort nok med vannsikkerheten*, 17.06.17, https://www.aftenposten.no/osloby/i/O1nV/Alsabeehg---Byradet-har-ikke-gjort-nok-med-vannsikkerheten

Kripos, Trendrapport 2016 – *Organisert og annen alvorlig kriminalitet i Norge*, 2016

Larsen, Heidi Elisabeth, Politiet ber om tips: *Politiet tror denne vannsabotøren har terrorisert kommunen i åtte år. Nå ber de om hjelp for å stoppe «vannmannen»* i Dagbladet, 11.09.2017. Tilgjengelig på: https://www.dagbladet.no/nyheter/politiet-tror-denne-vannsabotoren-har-terrorisert-kommunen-i-atte-ar-na-ber-de-om-hjelp-for-a-stoppe-vannmannen/68683035

Lia, Brynjar og Petter Nesser, *«Terror mot drikkevann – En oversikt over terrorgruppers interesse for å ramme offentlig drikkeforsyning»*, FFI-rapport: 2003/01919

Mattilsynet, Veiledning til drikkevannsforskriften, 2017

Mattilsynet, *Økt sikkerhet og beredskap i vannforsyningen* – fra ROS til operativ beredskap (veiledning), 2017

Norsk vann, *Sikkerhetsstyring for vannbransjen*, Norsk vann-rapport: 213/2015, 2015

Norsk vann, *Sikkerhet og sårbarhet i driftskontrollssystemer for VA-anlegg*, Norsk vann-rapport: 195/2013

NOU 2006: 6 *Når sikkerheten er viktigst — Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner*

NOU 2000: 24 *Et sårbart samfunn — Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet*

NSM, Veileder til objektsikkerhetsforskriften, 2014

NSM, Veiledning i verdivurdering, 2009

Politiet, NSM, Næringslivets sikkerhetsråd og PST, *Sikkerhet ved ansettelsesforhold – før, under og ved avvikling*, 2017

PST, Trusselvurdering 2017, 2017

PST, *Vurdering av trusselbildet – november 2017*, 22.11.17, Tilgjengelig på: https://www.pst.no/alle-artikler/pressemeldinger/vurdering-av-trusselbildet-i-norge---november-2017/

Reichborn-Kjennerud, Erik og Patrick Cullen, «What is Hybrid Warefare» i Policy Breif 1/2016, NUPI, 2016

Smith, C. og D. Brooks, Security science. The therory and Practice of security, Oxford: Elsevier, 2013

TIDLIGERE UTGITTE RAPPORTER

2017
- 228 Tilførsel av industrielt avløpsvann
- 227 Beregning av forurensningsutslipp fra avløpsanlegg
- 226 Tømming av slam
- 225 Trykkavløp i spredtbygde og urbane strøk
- 224 Eierskap til stikkledninger

2016
- 223 Finansieringsbehov i vannbransjen 2016–2040
- 222 Dokumentasjon av utslipp fra avløpsnettet
- 221 Smart ledningsfornyelse – bruk av NoDig-metoder
- B21 Utvikling av studietilbud i bachelor i vann- og miljøteknikk
- B20 Norske tall for vannforbruk med fokus på husholdningsforbruk
- 220 Kritiske ledninger for vann og avløp – klassifisering og tiltaksvurdering
- 219 Eksempler på implementering av bærekraft i vannbransjen
- 218 Vann til brannslokking og sprinkleranlegg
- 217 Videreutvikling av beregningsmetodikk for gjenanskaffelsesverdi og investeringsbehov

2015
- 215 Tilbakestrømssikring – veiledning til vannverkseiere
- 214 Forslag til ny sektorlov for vanntjenester
- 213 Sikkerhetsstyring for vannbransjen
- 212 Veiledning for dimensjonering av vannbehandlingsanlegg
- 211 Erfaringer med ozon-biofiltrering for behandling av drikkevann
- 210 Veiledning for praktisering av selvkost

2014
- 209 Veiledning i mikrobiell barriere analyse
- 208 Sikring av kvalitet på ledningsanlegg
- 207 Stikkledninger – ansvar og teknisk utforming
- 206 Biostabilitet i drikkevannsnett
- 205 Bærekraftig forvaltning av VA-tjenestene
- 204 Åpne flomveger i bebygde områder
- 203 Fra driftsassistanser til regionale vannassistanser
- 202 Microbial barrier analysis (MBA) – a guideline
- 201 Anskaffelser i vannbransjen
- 200 Håndtering av overvann fra urbane veger

2013
- 199 Etablering av gode VA-løsninger i spredt bebyggelse
- 198 Organiske miljøgifter i norsk avløpsslam – Resultater fra undersøkelsen i 2012/13
- 197 Avløpsanlegg Vurdering av risiko for ytre miljø
- 196 Veiledning i tilstandskartlegging og fornyelse av VA-transportsystemer
- 195 Sikkerhet og sårbarhet i driftskontrollsystemer for VA-anlegg
- B19 Varmepumper i drikkevannsforsyningssystem
- B18 Kranvannets kokebok for kommunikasjon
- B17 Investeringsbehov i vann- og avløpssektoren

2012
- 194 Energiriktig design og prosjektering av avløpsrenseanlegg
- 193 Veiledning i dimensjonering og utforming av VA-transportsystem
- 192 Veiledning for valg av riktige sensorer og måleutstyr i VA-teknikken
- 191 Rettigheter til uttak av vann til allmenn vannforsyning
- 190 Klimatilpasningstiltak innen vann og avløp i kommunale planer
- 188 Veiledning for drift av koaguleringsanlegg
- C8 Omdømmeplattform og -strategi

2011
- 187 Kommunal overtakelse av vannverk organisert som andelslag eller samvirkeforetak
- 186 Veiledning i omorganisering av andelsvannverk til samvirkeforetak
- 185 Fett i avløpsnett. Kartlegging og tiltaksforslag
- 184 Tilsyn med utslipp fra avløpsanlegg innen kommunens myndighetsområde
- 183 Veiledning om regulering av VA-tjenester til næringsmiddelindustri
- 182 Prøvetaking av avløpsvann og slam
- 181 Veiledning i bygging og drift av drikkevanns-basseng
- 180 Fjernavlesning av vannmålere
- 179 Veiledning i utarbeidelse av kommunale gebyrforskrifter for vann og avløp
- B16 Veiledning for kartlegging av energibruk i VA-sektoren
- B15 Vannforskriftens økonomiske konsekvenser for kommunesektoren og avløpsanleggene
- C7 Forvaltningspraksis ved norsk damsikkerhet

2010
- 178 Grunnundersøkelser for infiltrasjon – mindre avløpsanlegg
- 177 Drikkevannskvalitet og kommende utfordringer - problemoversikt og status
- 176 Statlige gebyrer og avgifter på de kommunale VAR-tjenestene
- 175 Vann og avløp for nye i bransjen – læreplan. E-læring og samlinger
- 174 Hygienisering av avløpsslam. Langtidslagring og enkel rankekompostering. Resultater fra 3 års valideringstesting
- 173 Veiledning for bruk av støpejernsrør
- B14 Klimatilpasningstiltak i VA-sektoren – forprosjekt
- B13 Silslam – mengder, behandlingsløsninger og bruksområder. Forprosjekt.

2009
- 172 Trykktap i avløpsnett
- 171 Erfaringer med lekkasjekontroll
- 170 Veileder til god desinfeksjonspraksis
- 169 Optimal desinfeksjonspraksis fase 2
- 168 Veiledning for dimensjonering av avløps-renseanlegg
- 167 Veiledning for kjøp av VA-kjemikalier
- 166 Tiltak for å bedre fosforfjerningen på kjemiske renseanlegg
- 165 Innsamlingsverktøy for vedlikeholdsdata
- B12 Drikkevatn i media

2008
- 164 Veiledning for UV-desinfeksjon av drikkevann
- 163 Veiledning for innhenting og evaluering av tilbud på analyseoppdrag
- 162 Veiledning i klimatilpasset overvannshåndtering
- 161 Helsemessig sikkert vannledningsnett
- 160 Driftserfaringer med membranfiltrering
- 159 Håndbok i kildesporing i avløpssystemet
- 158 Termoplastrør i Norge – før og nå
- B11 Økonomiske forhold i interkommunalt VA-samarbeid – praksis og kjøreregler
- B10 Vannkilden som hygienisk barriere
- B9 Utvikling av et system for spørreundersøkelser blant VA-kundene
- C6 I veien for hverandre – Samordning av rør og kabler i veigrunnen

2007
- 157 Organiske miljøgifter i norsk avløpsslam. Resultater fra undersøkelsen i 2006/07
- 156 Veiledning for oljeutskilleranlegg
- 155 Norm for merking og FDV-dokumentasjon i VA-sektoren
- 154 Norm for tagkoding i VA-anlegg
- 153 Norm for symboler i driftskontrollsystemer for VA-sektoren
- 152 Veiledning for anskaffelse av driftskontroll-systemer i VA-sektoren
- 151 Veiledning for vedlikeholdssystemer (FDV)
- 150 Dataflyt – Klassifisering av avløpsledninger
- B8 Forprosjekt energinettverk i VA-sektoren
- B7 Sandnesmodellen. Eksempel på system for kommunikasjon og virksomhetsstyring

2006
- 149 Tilførsel av industrielt avløpsvann til kommunalt nett. Veiledning
- 148 Veiledning i utarbeidelse av prøvetakings-programmer for drikkevann
- 147 Optimal desinfeksjonspraksis for drikkevann
- 146 Bærekraftig vedlikehold. Betraktninger av utvalgte problemstillinger knyttet til langsiktig forvaltning av vannledningsnett
- B6 Kommunikasjonsstrategi for NORVAR og norske vann og avløpsverk
- B5 Utslipp fra bilvaskehaller
- B4 Vannkvalitet i ledningsnett – Problemoversikt og statur. Forprosjekt.
- B3 Kvalitetsheving av nye VA-ledningsanlegg. Kartlegging og tiltaksforslag
- C5 Økt sikkerhet og beredskap i vannforsyningen – veiledning
- C4 Effekter av bruk av matavfallskverner på ledningsnett, renseanlegg og avfallsbehandling

2005
- 145 Inspeksjonsmanual for avløpssystemer. Del 1 – Ledninger
- 144 Veiledning i overvannshåndtering (Erstattet av 162/08)
- 143 Kartlegging av mulig helserisiko for abonnenter berørt av trykkløs vannledning ved arbeid på ledningsnettet
- 142 NORVARs benchmarkingsprosjekt 2004 Presentasjon av målesystem og resultater for 2003 ed analyse av datamaterialet
- B2 PressurePuls for deteksjon av lekkasje på vannledninger.
- C3 Samarbeid om økt bruk av avløpsslam på grøntarealer

2004
- 141 Trenger Norge en VA-lov? Drøfting av behovet for en egen sektorlov for vann og avløp
- 140 NORVARs videre arbeid med slam. Strategisk plan for prosjektvirksomhet, informasjon og kommunikasjon. Forprosjekt
- 139 Erfaringar med klorering og UV-stråling av drikkevatn
- 138 Veiledning for kontrahering av rådgivnings- og prosjekteringstjenester innen VAR-teknikk. Revidert utgave
- 137 Veiledning i bygging og drift av drikkevanns-basseng (Erstattet av 181/2011)
- 136 Hygienisk barrierer og kritiske punkter i vannforsyningen: Hva har gått galt?
- 135 Vannledningsrør i Norge. Historisk utvikling. 26 dimensjonstabeller
- 134 VA-JUS. Etablering og drift av vann- og avløpsverk sett fra juridisk synsvinkel (Erstattet av boken Vann- og avløpsrett (2010) og nettportalen va-jus.no)
- B1 Effektive VA-organisasjoner og tilfredse brukere. Forprosjekt
- C2 Stoff for stoff – kilde for kilde. Kvikksølv i avløpsnettet

2003
- 133 IT-strategi for VA-sektoren. Veiledning
- 132 Forslag til nytt system for prosjektvirksomheten i NORVAR
- 131 Effektivisering av avløpssektoren
- 130 Gjenanskaffelseskostnadene for norske VA-anlegg
- 129 Rørinspeksjon med videokamera. Veiledning/ rapportering hovedledninger
- C1 Sårbarhet i vannforsyningen

2002
- 128 Bruk av resultatindikatorer og benchmarking i effektivitetsmåling av kommunale VA-virksom-heter. Erfaringer og anbefalinger fra et prøveprosjekt
- 127 Vassdragsforbund for Mjøsa og tilløpselvene – en samarbeidsmodell
- 126 Organisering og effektivisering av VA-sektoren. En mulighetsstudie
- 125 Mal for forenklet VA-norm
- 124 Nødvendig kompetanse for legging av VA-ledninger. Læreplan for ADK 1
- 123 Utslipp fra mindre avløpsanlegg. Veiledning for utarbeidelse av lokale forskrifter (Utgått)
- 122 Prosessen ved utarbeidelse av miljømål for vannforekomster. Erfaringer og råd fra noen kommuner
- 121 Kjøkkenavfallskverner for håndtering av matavfall. Erfaringer og vurderinger
- 120 Strategi for norske vann- og avløpsverk. Rapport fra strategiprosess 2000/2001

2001
- 119 Omstruktureringer i VA-sektoren i Norge En kartlegging og sammenstilling
- 118 Veiledning for kontrahering av rådgivnings- og prosjekteringstjenester innen VAR- teknikk (Erstattet av 138/04)
- 117 VA-juss. Etablering og drift av vann- og avløpsverk sett fra juridisk synsvinkel (Erstattet av 134/03)
- 116 Scenarier for VA-sektoren år 2010
- 115 Pumping av avløpsslam. Pumpetyper, erfaringer og tips
- 114 Nødvendig kompetanse for drift av vannbehand-lingsanlegg. Læreplan for driftsoperatør vann
- 113 Nødvendig kompetanse for drift av avløpsrense-anlegg. Læreplan for driftsoperatør avløp
- 112 Erfaringer med nye renseløsninger for mindre utslipp

2000
- 111 Eksempel på driftsinstruks for silanlegg. Cap Clara i Molde kommune
- 110 Veileder i konkurranseutsetting. Avtaler for drift og vedlikehold av VA-anlegg
- 109 Resultatindikatorer som styringsverktøy for VA-ledelsen
- 108 Data for dokumentasjon av VA-sektorens infrastruktur og resultater
- 107 Utslipp fra mindre avløpsanlegg. Teknisk veiledning. Foreløpig utgave
- 106 Effektiv bruk av driftsinformasjon på rense-anlegg/mal for rapportering
- 105 Sjekkliste plan- og byggeprosess for silanlegg
- 104 Nordisk konferanse om nitrogenfjerning og biologisk fosforfjerning 1999
- 103 Returstrømmer i renseanlegg. Karakterisering og håndtering

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