Sikring av kritisk VA-infrastruktur mot digitale og fysiske trusler: STOP-IT-metoden demonstrert og testet i et vannverk

Av Camillo Bosco, Gema Raspati, Kebebe Tefera, Harald Rishovd og Rita Ugarelli

Camillo Bosco (Ph.D) er forsker i SINTEF Community.
Gema Raspati (Ph.D) er forsker i SINTEF Community.
Kebebe Tefera (M.Sc) er overingeniør i Oslo kommune, Vann- og avløpsetaten.
Harald Rishovd (M.Sc) er seniorkonsulent i Oslo kommune, Vann- og avløpsetaten.
Rita Ugarelli (Ph.D) er sjefsforsker i SINTEF Community og professor II ved NTNU.

Summary

Securing critical water infrastructure against digital and physical threats: the STOP-IT method demonstrated and tested in a waterworks. Water critical infrastructures are undergoing a process of digital transformation which entails an increasing integration between the physical and cyber layers of the system. This integration brings efficiency and monitoring advantages, but it also exposes water systems to a new threat surface that includes cyber-attacks. Formed in 2017, STOP-IT is Europe's first project dedicated to developing cyber-physical security solutions tailored to the water sector. During the four years of collaboration, the STOP-IT team has co-developed an extensive list of technologies that integrates cyber and physical layers of infrastructure, allowing water utilities to prevent, detect, assess, and treat risks, as well as simulate scenarios of attacks and explore how to react to increase preparedness. This article first introduces the overall aim and main outcomes of the STOP-IT project and then focuses on the risk management integrated framework composed of modelling solutions developed to help water utilities identify vulnerabilities and protect critical parts of their systems. The solutions are presented along with the results from the demonstration activities performed by a selected water utility.

Sammendrag

Kritisk vanninfrastruktur gjennomgår en digital transformasjon som innebærer økt integrasjon mellom fysiske og digitale komponenter i systemet. Samhandlingen gir bedre effektivitet og overvåking av VA-systemet, men innebærer også nye trusler, inkludert cyberangrep. STOP-IT startet i 2017 og er Europas første prosjekt for å utvikle skreddersydde digitale og fysiske sikkerhetsløsninger for vannsektoren. I løpet av et fireårig samarbeid har STOP-IT-teamet utviklet en rekke løsninger som kombinerer digital og fysisk infrastruktur, slik at vannverk kan forebygge, oppdage, vurdere og behandle risikoer. De kan også simulere scenarier for angrep og undersøke hvordan man kan øke beredskapen. Denne artikkelen presenterer først det overordnede målet og hovedresultatene fra STOP-IT. Deretter fokuserer den på rammeverket for risikostyring som består av modelleringsløsninger som skal hjelpe vannverk med å identifisere sårbarheter og beskytte kritiske

deler i systemene. Løsningene presenteres sammen med resultater fra demonstrasjonen som ble utført ved et vannverk.

Innledning

Forvaltningen av urbane vannsystemer utfordres av flere faktorer, som aldrende infrastruktur, store lekkasjer, økt press på vannressursene, både mengde og kvalitet. Disse faktorene forverres av globalt press, som befolkningsvekst, økt etterspørsel etter vann, byutvikling, urbanisering og klimaendringer. I tillegg kommer nye og eksiterende lover og regler for vannkvalitet, sikkerhet og miljøhensyn. Disse faktorene er til sammen drivere for et paradigmeskifte innen vannforvaltningen der en digital transformasjon legger grunnlaget. Digitaliseringen går langsommere i vannsektoren enn i andre kritiske infrastruktursektorer, blant annet på grunn av sikkerhetsutfordringer. Sikkerhet har vært høyt prioritert i vannsektoren i årevis, og cybersikkerhet blir en stadig større utfordring. Likevel mangler vi tiltak og tilnærminger som tar hensyn til den globale sikkerhetskonteksten, fysisk som digital. Resultatet er manglende evne til å takle alvorlige cyber-fysiske angrep.

Vannsektoren mangler en felles forståelse av cybertruslene. En systematisk deling av informasjon om cyberangrep mellom vannverk og IT-leverandører kunne bidratt til en bedre vurdering av cybersikkerheten i vannsektoren, økt beredskap og mulighet til å sikre tjenestene.

STOP-IT har jobbet i flere retninger for å bidra til økt sikkerhet for vann som en kritisk infrastruktur: på den ene siden har det blitt gjort innsats for å øke bevisstheten og kompetansen blant operatørene, og på den andre siden for å tilby fleksible og tilpasningsdyktige løsninger [Ugarelli et al., 2021].

Det teknologiske resultatet av prosjektet er STOP-IT-plattformen som inneholder 28 løsninger som kan brukes hver for seg eller sammen. Brukerne kan velge teknologier som er relevante for deres spesifikke utfordringer, samtidig som det er mulig å legge til komponenter for å styrke beskyttelsen mot cyber-fysiske trusler etter behov, og analysere gjennomgripende effekter av fysiske hendelser og cyberhendelser.

Denne artikkelen presenterer de strategiske og taktiske verktøyene fra STOP-IT og hvordan de er tilpasset og testet for å beskytte et vannforsyningssystem.

Metode

Studien brukte den strategiske og taktiske løsningen: *Risk Analysis and Evaluation Toolkit* (RAET) [Makropoulos et al., 2019a]. RAET er en helhetlig integrert plattform som skal hjelpe vannverk med å håndtere cyber-fysiske risikoer for kritiske systemer og tjenester, og forsterke motstandsdyktigheten (”resilience”) [Makropoulos et al., 2018; Nikolopoulos et al., 2019] i vannsektoren.

RAET bygger på risikostyringsprosessen beskrevet i ISO 31000:2009/2018 (den definerer trinnene for risikoidentifikasjon, analyse, evaluering og tiltak) og tilpasser trinn og metode til cyber-fysisk sikkerhet. Rammeverket inneholder:

- *Asset Vulnerability Assessment to risk events Tool* (AVAT) [Ostfeld et al., 2018] viser hvor kritisk hvert element i vannledningsnettet er ved å bruke sårbarhetsindekser som, for eksempel *Link Criticality Index*, dvs. antall frakoblede noder etter avbrudd. Verktøyet bidrar til å håndtere kompleksiteten i vannledningsverk, hvor det vanligvis ikke er enkelt å identifisere de mest sårbare komponentene. Verktøyet kan vurdere systemets sårbarhet for ulike konfigurasjoner av nettverket, og rangere ledningene etter hvor store konsekvenser det har for systemet om det oppstår feil på ledningen. [Raspati et al., 2022].
- En scenarioplanlegger [Makropoulos et al., 2019b] som hjelper brukeren med å lage angrepsscenarier. Planleggeren støttes av en risikoidentifikasjonsdatabase (RIDB) hvor potensielle risikohendelser kan velges, og STOP-IT feiltrær (FT-er) for å navigere gjennom flere veier fra trusler til hendelser. Angrepsscenarioene kan deretter undersøkes og simuleres videre i *Stress Testing Platform*.
- En avansert verktøykasse [Makropoulos et al., 2019b] for analyse og evaluering av risikoer for vannsystemet som omfatter noen

Tabell 1. Sammendrag av utvalgte risikoscenarioer valgt av vannverket for RAET-demonstrasjonen

#	Navn på scenario	Beskrivelse
1	Risikoscenario 1	*Cyber-fysisk manipulering av kontrollsystem som påvirker høydebasseng*
2	Risikoscenario 2	*Risikoscenario 1 kombinert med fysisk ødeleggelse av høydebasseng eller ledning*
3	Risikoscenario 3	*Manipulering av nivåsensor i høydebasseng som brukes til brannslokking*

av de nyeste modellene og verktøyene. Verktøykassen etterligner vanndistribusjonssystemet som en cyberfysisk modell og vurderer virkningen av potensielle hendelser som følge av cyber-fysiske trusler. Resultatene visualiseres i det såkalte KPI-verktøyet (*Key Performance Indicator tool*). Verktøykassen simulerer effekter både på vannmengde og vannkvalitet.

- En *Risk Reduction Measures Database* (RRMD) [Mälzer et al., 2018] med avanserte funksjoner for å identifisere riktig risikoreduserende tiltak (RRM). RRMD er koblet til RIDB. RRMD er implementert i STOP-ITs risikostyringsprosess for å hjelpe med å velge og vurdere effektiviteten av risikoreduserende tiltak for å øke systemets ytelse under et gitt angrepsscenario.
- En *Stress Testing Platform* (STP) [Ahmadi et al., 2019, Nikolopoulos et al., 2020] som kan simulere både fysiske og digitale systemer. STP kobler simuleringsmiljøet for det fysiske laget til et simuleringsmiljø som er i stand til å modellere cyberlaget i vannsystemets kontroll- og kommunikasjonsinfrastruktur (f.eks. fra SCADA til PLSer til overvåking), hvor cyberbeskyttelsesløsninger blir implementert og cyberangrep simulert. Plattformen gjør det mulig å analysere for eksempel effektene av skadevare i kontrollsystemet og hvordan de påvirker KPI-ene.

STOP-IT RAET-verktøykassen ble testet og demonstrert i et vannverk som er partner i prosjektet. Målet var å undersøke om det er forhold i vannledningsnettet som kan hindre god nok levering av vann til kunder og brannslokking. Følgende risikohendelser ble valgt for å evaluere konsekvensene i en detaljert risikovurdering:

- Manipulering av høydebassengets nivåsensorer ved cyberangrep eller fysiske angrep. Drift av pumper og ventiler i systemet styres ofte av vannivået i bassengene. Hvis sensorene ikke leser av riktig nivå, kan pumpen og/eller ventilen forhindre at nettet leverer nødvendig vannmengde både ved normal drift og til brannslokking.
- Kritisk svikt på ledning som følge av et målrettet fysisk angrep. Hendelsen analyserer svikt i en kritisk ledning i systemet. Konsekvensene forplanter seg mot forsyningsområdet i form av potensielt lavt trykk som igjen kan føre til ikke-levert vann, spesielt hvis det er kombinert med manipulering av vannnivå-sensoren i et høydebasseng.

Basert på de to nevnte risikohendelsene ble risikoscenarioene bygget med scenarioplanleggeren (RIDB og FT) som beskrevet i Tabell 1. De tre risikoscenarioene i er «hva-om»-scenarioer, typiske for planleggingsfasen. Tilpasning til det aktuelle ledningsnettet og etterfølgende konsekvensutredning utføres med RAET.

Resultater og diskusjon

De tre risikoscenarioene ble benyttet av vannverket for å teste RAET. De brukte en tilgjengelig hydraulisk modell for en del av vannledningsnettet. Modellen forsyner ca 92 000 innbyggere. Total ledningslengde er 250 km og består av 5482 ledninger og 5223 knutepunkt (noder).

EPANET 2.2 ble brukt som beregningsmotor for den hydrauliske modellen. Scenariene ble vurdert ved å bruke forskjellige moduler i RAET.

Fra feiltrærne foreslås en liste med mulige hendelser. Hendelse 235 ”En uvedkommende

person på stedet manipulerer høydebassengets nivå-måler" ble valgt, se figur 1. I scenarioplanleggeren ble verktøyet RISKNOUGHT [Nikolopoulos et. al., 2020] valgt for simuleringen. For å simulere et angrepsscenario var det først nødvendig å definere et Business as Usual (BaU)-scenario uten angrep. En Extended Period Simulation (EPS) av BaU-scenario ble kjørt gjennom scenarioplanleggeren. Deretter ble angrepsscenarioet opprettet ved legge til Hendelse 235 fra brukergrensesnittet. For den valgte hendelsen velges ett av disse tre høydebassengene (HB) i ledningsnettet:

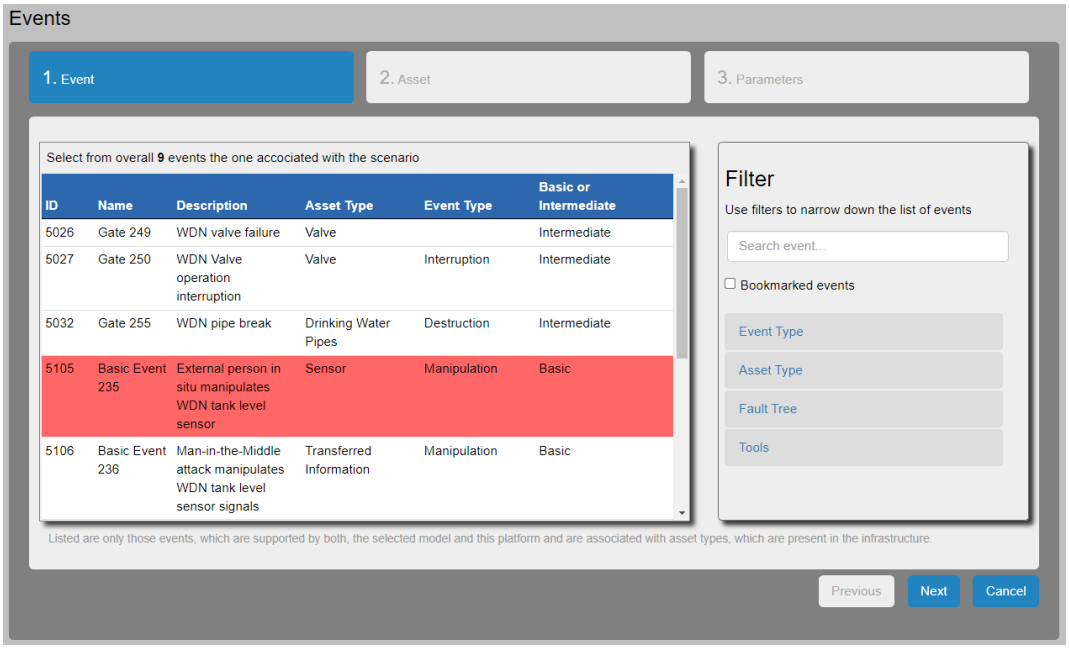
- HB 1: hoved-høydebasseng, direkte koblet til kilden, til hele ledningsnettet og til HB 2.
- HB 2: høydebasseng som leverer vann til høyereliggende områder.
- HB 3: brukes hovedsakelig som lagring med tanke på brannslokking i et område.

Scenario 1

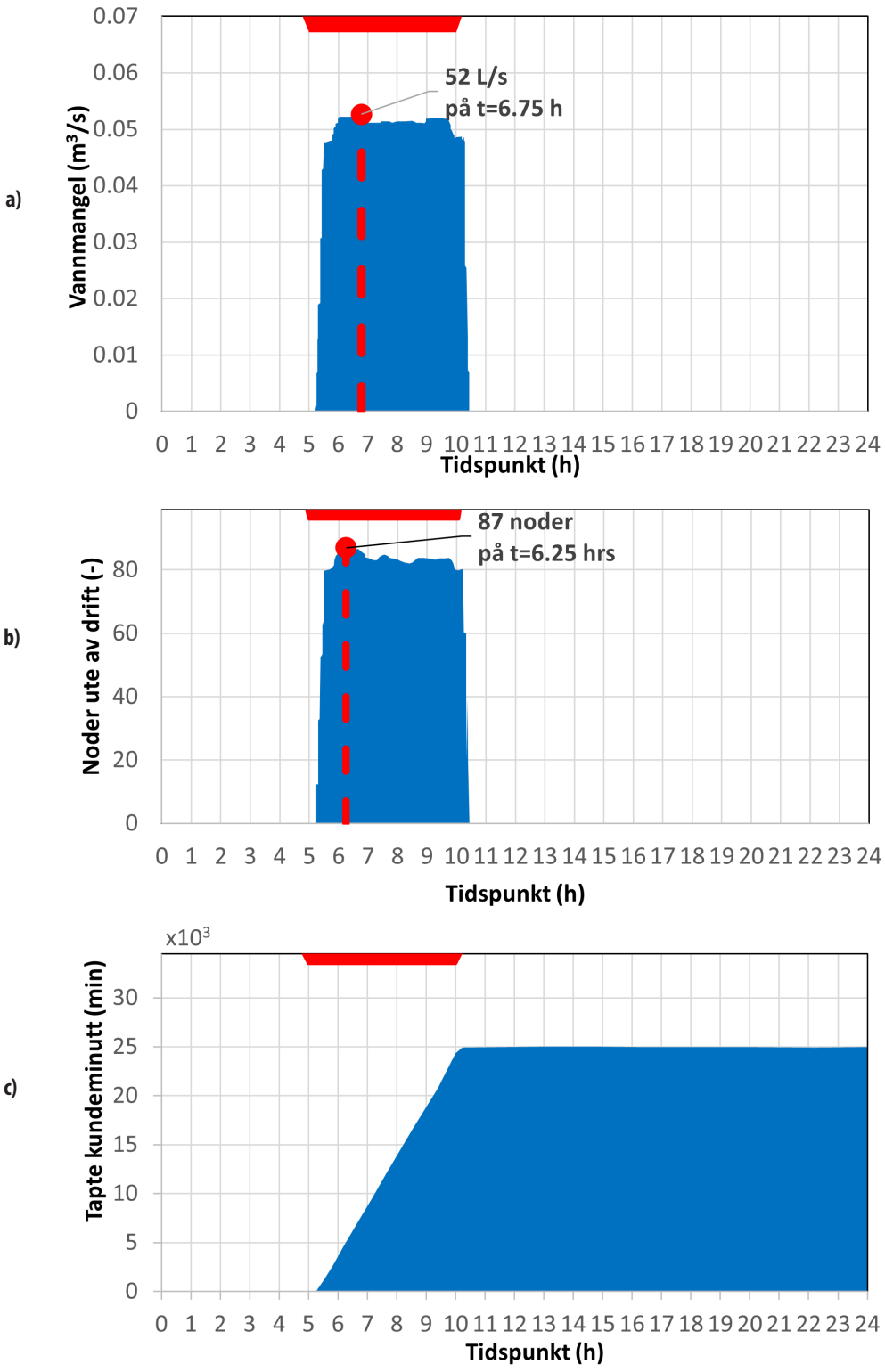
Målet med vurderingen av risikoscenario 1 var å identifisere områder med manglende levering ved manipulering av nivåavlesninger og HB 2 ble valgt for å finne ut hvor store områder som er strengt avhengige av bassenget. Tre parametere måtte defineres: varighet av angrepet, starttidspunkt for angrepet og det manipulerte vannivået i bassenget. Angrepets varighet ble satt til 5 timer, starttiden til kl. 05.00 og den manipulerte vannstand til 10 meter som er maksimumsnivået for HB 2 og som gjør at pumpen som kobler HB 1 til HB 2 settes ut av drift. Figur 1 viser risikohendelsen i scenarioplanleggeren.

Simuleringen av risikoscenario 1 ga kunnskap om hvilke områder som får de mest alvorlige konsekvensene ved manipulering av sensoravlesninger av nivået i HB 2. Konsekvensene ble vurdert ved å bruke KPI-verktøyet, hvor påvirkningen ble vurdert etter størrelsen på det kritiske området og ikke-levert vann.

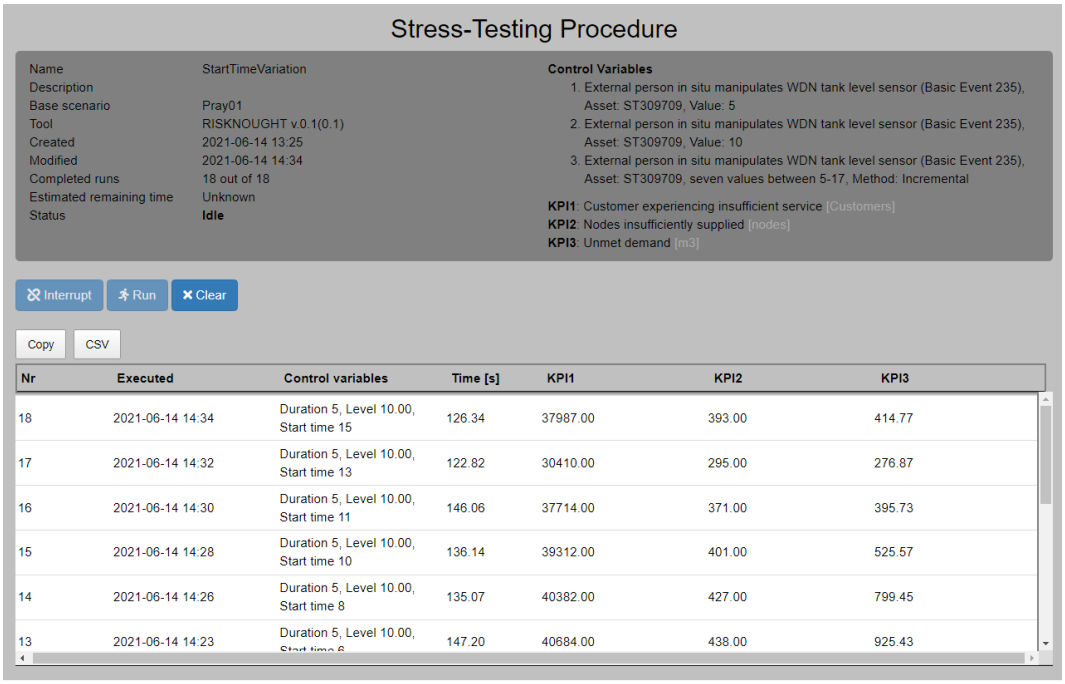
Figur 2 (a) viser ikke-levert vannmengde mellom kl. 05.00 og kl. 10.00, som en konsekvens av angrepet. Ikke-levert vannmengde er størst rundt kl. 07.00 når de fleste forbrukene starter dagen. Ikke-levert vannmengde er da nesten konstant på 50 l/s. Figur 2 (b) viser at antall noder ute av drift likner grafen for ikke-levert vann, og den viser også at nesten hele området forblir uten vann. Antall kundeminutter (=antall minutter*antall berørte) øker lineært med tiden, til slutten av angrepet, se figur 2 (c).



Figur 1. Valgt risikohendelse for risikoscenario 1 foreslått av feiltreet i scenarioplanleggeren



Figur 2. Ikke-levert vann (a), antall noder ute av drift (b) og antall kundeminutter (c) for risikoscenario 1



Nr	Executed	Control variables	Time [s]	KPI1	KPI2	KPI3
18	2021-06-14 14:34	Duration 5, Level 10.00, Start time 15	126.34	37987.00	393.00	414.77
17	2021-06-14 14:32	Duration 5, Level 10.00, Start time 13	122.82	30410.00	295.00	276.87
16	2021-06-14 14:30	Duration 5, Level 10.00, Start time 11	146.06	37714.00	371.00	395.73
15	2021-06-14 14:28	Duration 5, Level 10.00, Start time 10	136.14	39312.00	401.00	525.57
14	2021-06-14 14:26	Duration 5, Level 10.00, Start time 8	135.07	40382.00	427.00	799.45
13	2021-06-14 14:23	Duration 5, Level 10.00,	147.20	40684.00	438.00	925.43

Figur 3. Oversikt over resultater i STP knyttet til risikoscenario 1

Risikoscenario 1 ble videre brukt for å teste Stress Testing Platform (STP) i RAET ved å variere en av de tre parameterne for den valgte hendelsen. Starttidspunktet ble økt jevnt fra kl. 05.00 til kl. 15.00 mens varigheten av angrepet ble opprettholdt på 5 timer. STP bidrar med ekstra innsikt fordi den gjør det mulig å se hvordan ulike inngangsverdier påvirker effekten angrepet har på systemet.

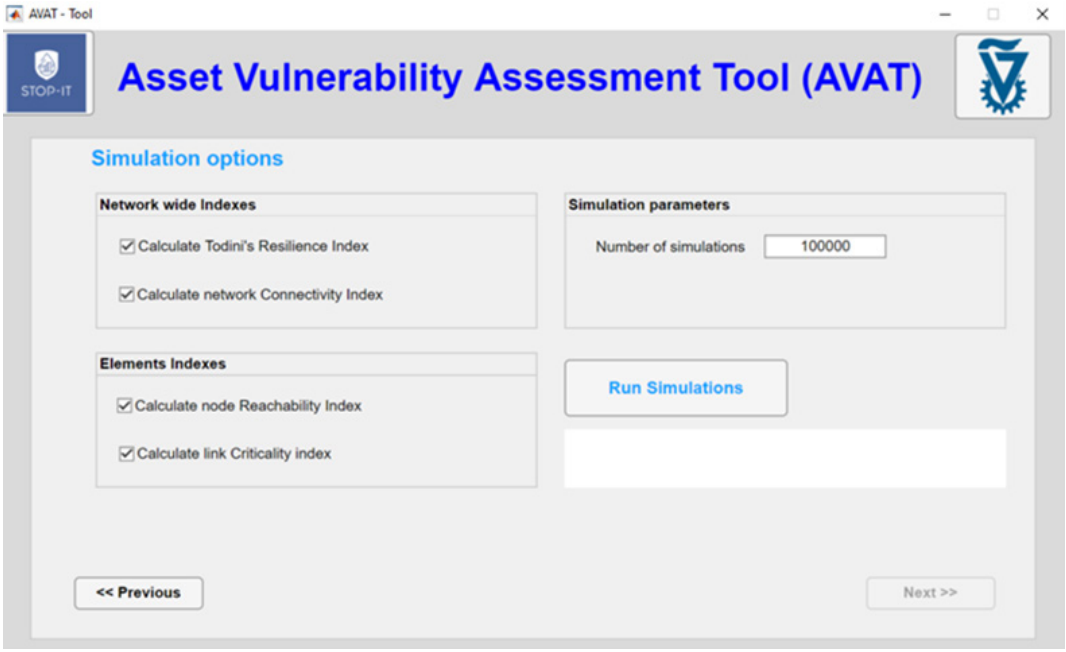
Figur 3 viser brukergrensesnittet til STP, der oppsummering av ulike KPIer er listet opp: "tapte kundeminutter" KPI 1, "Noder ute av drift" KPI 2, og "Ikke-levert vann" KPI 3. Simuleringene bekreftet at det mest kritiske tidspunktet på dagen er tidlig morgen.

Til slutt ble RRMD brukt for å identifisere tiltak som kan redusere risikoen forbundet med angrepet. Fysisk beskyttelse av området der HB 2 er plassert, vil redusere sannsynligheten for at uvedkommende kommer inn på området, og derfor ble følgende tiltak fra RRMD foreslått:

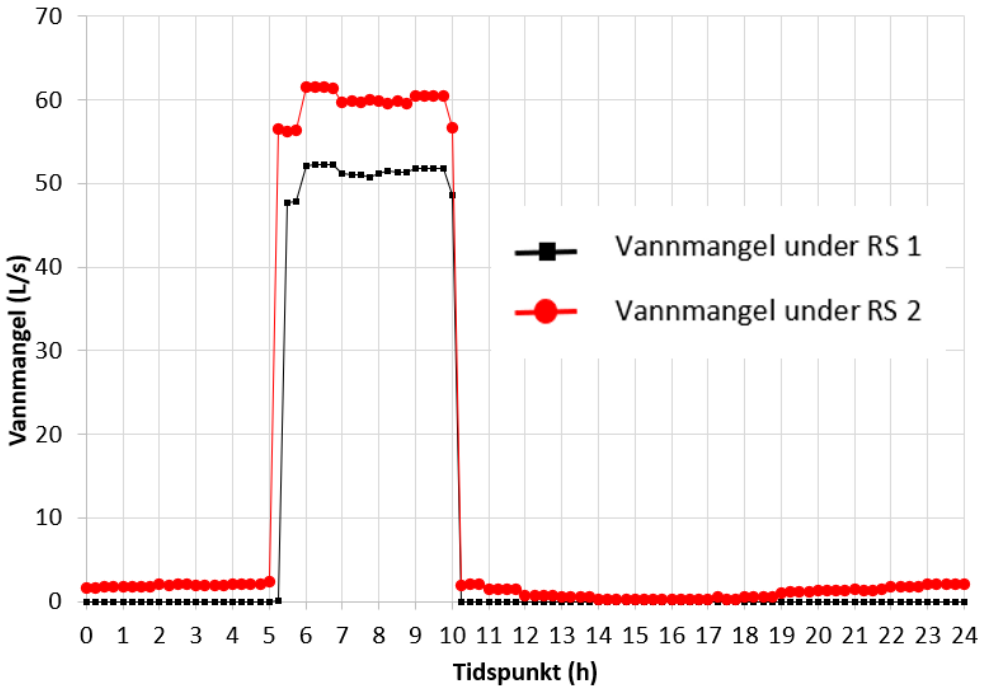
- M01: Gjerder og vegger rundt sensitive installasjoner (f eks høydebasseng)
- M02: Bevegelsesdetektorer
- M03: Kameraovervåking
- M04: Vaktpatruljer
- M07: Alarmsystemer
- M08: Sikre dører og vinduer
- M09: Adgangskontroll
- M10: Innbruddsikre dører/låser

Scenario 2

Risikoscenario 2 var en kombinasjon av risikoscenario 1 og i tillegg brudd på en kritisk ledning. Ledningen ble identifisert av verktøyet Asset Vulnerability Assessment to Risk Events (AVAT). Vannverket var allerede klar over at hovedledningen som var direkte knyttet til kilden var den mest kritiske, men det var usikkerhet rundt lokalisering av andre kritiske ledninger i distribusjonsnettet. AVAT beregnet Link Criticality Index som gjorde det mulig å fastslå viktigheten av de ulike komponentene for vannforsyningen og dermed hvor "attraktivt" det var å angripe dem. AVAT-demonstrasjonen bestod i å klargjøre to input-filer, en EPANET INP-fil og en Excel-fil med sannsynlighet for brudd for hver ledning. Figur 4 viser en vellykket opplasting av ledningsnettet i AVAT.



Figur 4. Simuleringsalternativer i AVAT



Figur 5. Ikke-levert vann ("Vannmangel") for risikoscenario 1 og risikoscenario 2

Etter at den kritiske ledningen var identifisert, ble trinnene fra Risikoscenario 1 gjentatt i scenarioplanleggeren. Den eneste forskjellen var at det ble lagt inn ledningsbrudd i simuleringen, i tillegg til manipulering av nivåsensoren. Hendelsen 255 "Brudd på vannledning" ble valgt.

For å simulere ledningsbruddet ble sprinkler-koeffisienten satt til 5. Det medførte en tilsynelatende stor lekkasje på ledningen.

I følge AVAT ble den mest kritiske ledningen i nettet, etter hovedledningen fra kilden, en ledning til et område med ensidig forsyning. I scenarioplanleggeren ble det lagt til brudd på denne ledningen i tillegg til angrepet fra scenario 1. Som forventet hadde manipulering av sensornivået i HB 2 en mye større virkning på nettet enn rørbruddet. Figur 5 viser at ledningsbruddet bare førte til en liten ekstra mengde ikke-levert vann sammenlignet med resultatene i risikoscenario 1.

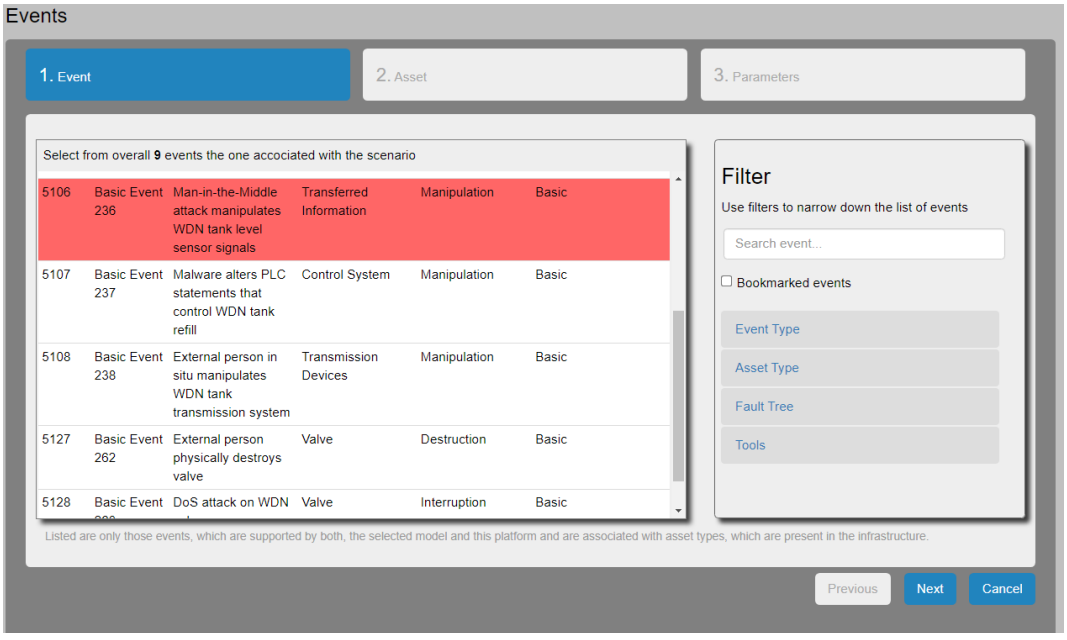
Basert på resultatene gjelder de relevante RRM-ene som ble identifisert for risikoscenario 1, også for risikoscenario 2.

Scenario 3

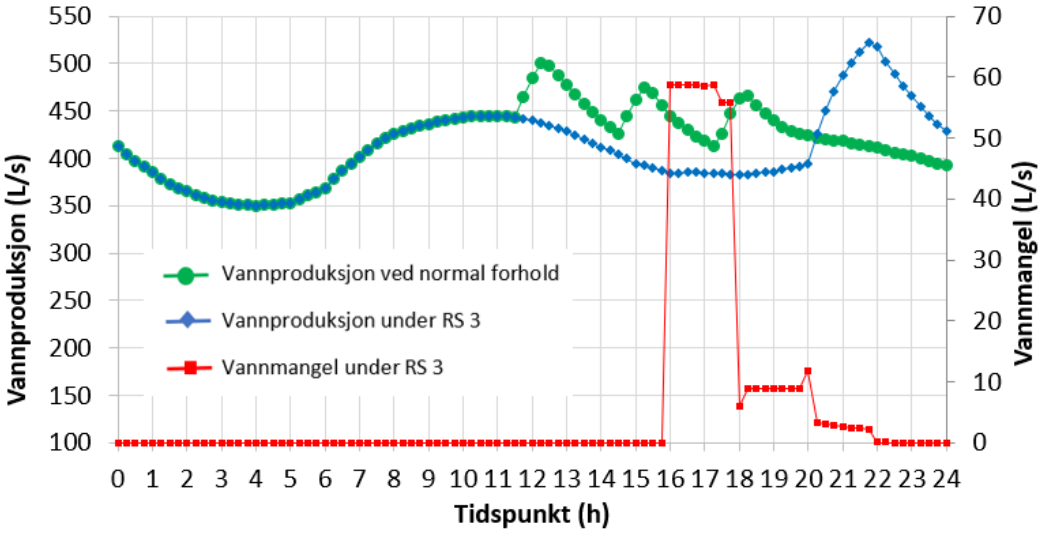
Risikoscenario 3 var konseptuelt likt risikoscenario 1, men nå ble Hendelse 236 "Man-in-the-middle-angrep manipulerer signalet fra høydebassengets nivåsensor" valgt fra feiltrærne. I scenarioplanleggeren ble RISKNOUGHT valgt, og et scenario med brannslokking ble analysert. Det ble satt inn et brannvanns-uttak på 50 l/s i den hydrauliske modellen for en kritisk sone i byen fra kl. 11.00 til 18.00. Ettersom HB 3 hovedsakelig fungerer som lagring for brannslokking i den aktuelle sonen, ble det valgt for å identifisere maksimum tid til reparasjon før det oppstod en situasjon med ikke-levert vann. Varigheten av cyberangrepet ble satt til 10 timer, starttiden til kl 10.00, og den manipulerte vannstanden til 6,5 meter (som var maksimalt nivå i HB 3, noe som førte til at ventilen som leverte vann forble stengt). Figur 6 viser et utvalg av risikohendelser fra scenarioplanleggeren.

Simuleringen av scenario 3 ga innsikt om hvor lang tid man har til å reparere skaden før det blir kritisk for systemet under brannslokking ved cyberangrep på sensoravlesningen til HB 3. Ikke-levert vann oppstår 5 timer etter at brannslokkingen starter. Figur 7 viser resultater for vannproduksjon og ikke-levert vann ved brannslokking.

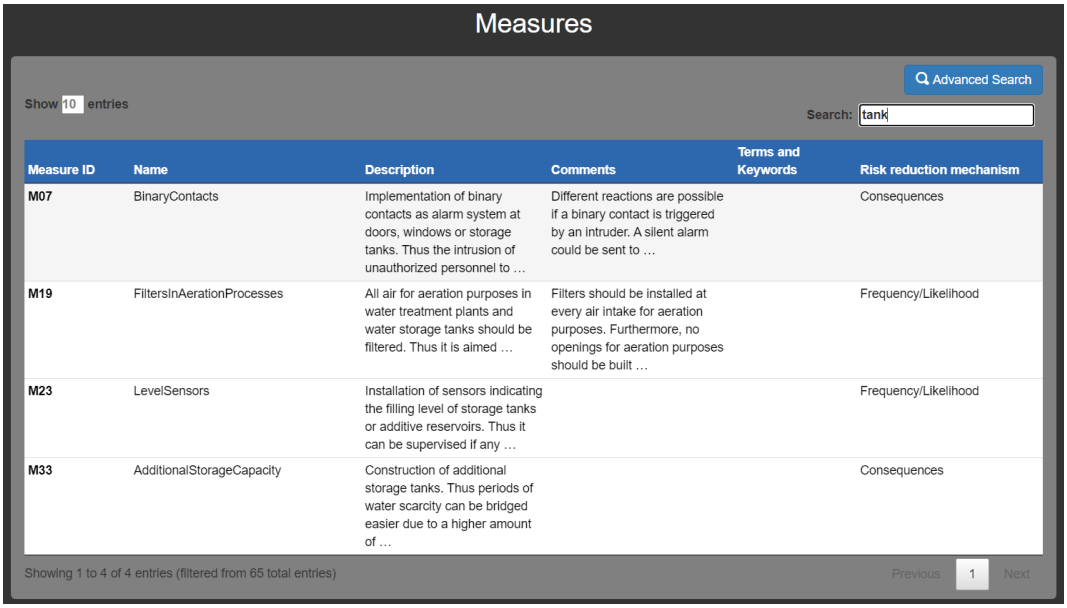
Fra figuren kan vi se at det lagrede volumet i HB 3 ikke var nok til å forsyne brannslokkingen i dette scenariet. Den sykliske prosessen med å fylle HB 3 startet rett etter klokken 11.00, og fra 16.00 til 18.00 kunne ikke vann til brannslok-



Figur 6. Valg av risikohendelse for risikoscenario 3 foreslått av feiltreet i scenarioplanleggeren



Figur 7. Resultater av risikoscenario 3 for vannproduksjon og ikke-levert vann



Figur 8. Brukergrensesnitt for RRMD

king leveres. Fra klokken 18 ble det antatt at brannslokkingen var over, men cyberangrepet pågikk i ytterligere to timer, dermed ble det noe ikke-levert vann fordi noen kunder i området forble uten vann til klokken 20, da cyberangrepet stoppet. Etter angrepet ble forsyningen til HB 3 gjenopprettet, og bassengfyllingen startet rett etter kl. 20. Ekstra lagring av vann til brannslokking kan velges som et risikoreduksjonstiltak, se EkstraLagringsVolum "AdditionalStorageCapacity" (M33) i RRMD i figur 8.

Konklusjoner

STOP-IT-prosjektet (2017-2021) hadde som mål å øke bevisstheten, kompetansen og beredskapen rundt cyber-fysisk beskyttelse av den kritiske infrastrukturen som vannforsyningen er. Artikkelen fokuserer på de teknologiske

resultatene av prosjektet, og spesielt på RAET-rammeverket som skal støtte vannverkenes strategiske og taktiske beslutninger. Ved å lage potensielle angrepsscenarier og teste ytelsen i systemet kan man ved hjelp av RAET undersøke muligheter for å øke beredskapen. Det gjør man ved å identifisere tiltak for risikoforebygging og risikoredusering, samt vurdere hvor mye tid man har til å reagere ved et angrep før systemet er alvorlig svekket. Innsikten som her er presentert og oppnådd ved å teste RAET i virkeligheten, har blitt svært godt mottatt av vannverket. De har bestemt seg for å ta i bruk RAET som en del av sin risikostyringspraksis, også etter at STOP-IT-prosjektet er avsluttet.

Takk til

STOP-IT-prosjektet har mottatt støtte fra EUs forsknings- og innovasjonsprogram Horizon 2020 (tilskuddsavtale nummer 740610).

Forfatterne takker for verdifull hjelp og bidrag fra alle samarbeidspartnere i prosjektet.

Referanser

Ahmadi M., Ugarelli R., Grøtan T. O., Raspati G.S., Selseth I., Makropoulos C., Nikolopoulos D., Moraitis G., Karavokiros G., Bouziotas D., Lykou A., Tsoukalas I. (2019) "Cyber – Physical Threats Stress – Testing Platform". Deliverable of STOP-IT Project D4.4.

Makropoulos C., Nikolopoulos D., Palmen L., Kools S., Segrave A. Vries D. Koop S. van Alphen H.J., Vonk E.; van Thienen P. (2018) "A resilience assessment method for urban water systems". Urban Water J., 15, 316–328, doi:10.1080/1573062X.2018.1457166.

Makropoulos C., Moraitis G., Nikolopoulos D., Karavokiros G., Lykou A., Tsoukalas I., Morley M., Gama M.C., Okstad E., Vatn J. (2019a) "Risk Analysis and Evaluation Toolkit". Deliverable of STOP-IT Project D4.2.

Makropoulos C., Moraitis G., Nikolopoulos D., Karavokiros G., Lykou A., Tsoukalas I., Morley M., Gama M.C., Okstad E., and Vatn J. (2019b) " Risk Analysis and Evaluation Toolkit." Deliverable of STOP-IT Project D4.2.

Mälzer H. J., Vollmer F., Corchero A. (2019) "Risk Reduction Measures Database (RRMD) supporting document". Deliverable of STOP-IT Project D4.3.

Nikolopoulos D., van Alphen H.J., Vries D., Palmen L., Koop S., van Thienen P., Medema G., Makropoulos C. (2019) "Tackling the "new normal": A resilience assessment method applied to real-world urban water systems". Water (Switzerland), 11, 330, doi:10.3390/w11020330.

Nikolopoulos D., Moraitis G., Bouziotas D., Lykou A., Karavokiros G., Makropoulos C. (2020) "Cyber-physical stress-testing platform for water distribution networks". Journal of Environmental Engineering, 146 (7), 04020061, doi:10.1061/(ASCE)EE.1943-7870.0001722,

Ostfeld A., Salomons E., Roth R., Zeevi G., Weiss H., Vatn J., Okstad E. (2018) "Asset Vulnerability Assessment to Risk Events". Deliverable of STOP-IT Project D4.1.

Raspati G. S., Bruaset S., Bosco C., Mushom L., Johannessen B., Ugarelli R. (2022) "A Risk-Based Approach in Rehabilitation of Water Distribution Networks". International Journal of Environmental Research and Public Health, 19(3), 1594.

Ugarelli R.M., Raspati G.S., Selseth I., Jaatun M.G., Røstum J., Rishovd H., Furuberg K. (2021). Cybersikkerhet i VA-sektoren og bidraget fra STOP-IT-prosjektet. VANN Volum 56.(3) s. 253-261