SINTEF

Kan vannet bli digitalt uten at det stopper?

Martin Gilje Jaatun

(Yaw-toon)

Martin.G.Jaatun@sintef.no

@seniorfrosk

@seniorfrosk@snabelen.no

STOP-IT-prosektet

- Gjør vann- og avløpssystemer sikrere og mer motstandsdyktige mot cyberfysiske trusler
  - bedre forberedelser
  - bevisstgjøring
  - forbedret hendelseshåndtering

STOP-IT-løsningene vil hjelpe VA-verk med å prioritere risikoer og utvikle en realistisk tilnærming og plan for forbedret fysisk/cyber beskyttelse

STOP-IT-videoen:
https://youtu.be/kG6lekwhmJo

Prosjektperiode: 2017-2021

Plattformen

- Skalerbar
  - Fra små til store vannverk
- Tilpasningsdyktig
  - Plukk og bland moduler etter behov
- Fleksibel
  - Kan brukes på forskjellige måter avhengig av brukergruppe

The Modules of STOP-IT platform

Modul 1: Strategiske og taktiske beslutnings-støtteverktøy

Modul 2: Verktøy for å detektere og varsle om trådløse jamme-angrep

Modul 3: Verktøy for å monitorer og beskytte SCADA/IT

Modul 4: Verktøy for å beskytte mot fysiske trusler

Modul 5: Verktøy for å dele informasjon om cybertrusler

Modul 6: Verktøy for å detektere cyber-fysiske uregelmessig-heter

Modul 7: Verktøy for å varsle innbyggere om kritiske situasjoner

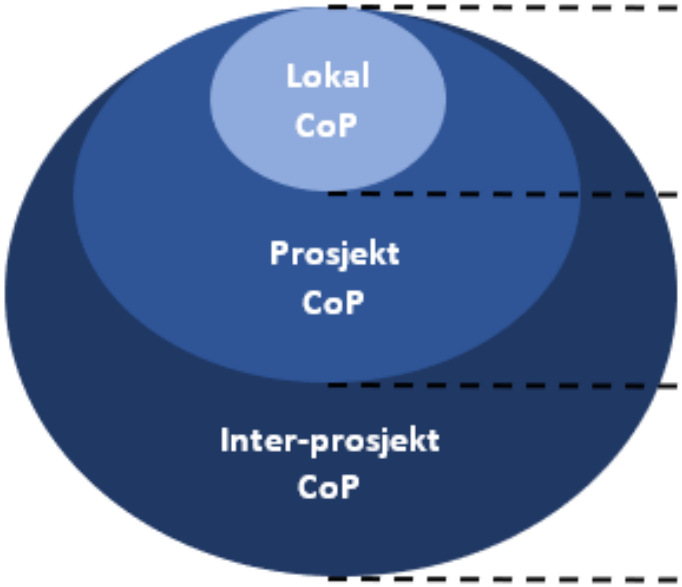
Modul 8: Verktøy for risikovurdering, varsling, og forslag til mottiltak

Modul 9: Verktøy for å visualisere informasjon fra alle de andre modulene

STOP-IT er mer enn bare teknologiske løsninger

- Samarbeid og bevisstgjøring
- Kompetanseutvikling
- Kommunikasjon og kunnskapsdeling
- Markedspåvirkning
- Påvirkning av retningslinjer og politikk
- Synergieffekter

Praksisfellesskap



Nivå: Vannverk
Kommunikasjon: Ekspertmøter som involverer relevante beslutningstakere og interessenter
Konfidensialitetsnivå: høy (kun fysiske møter)

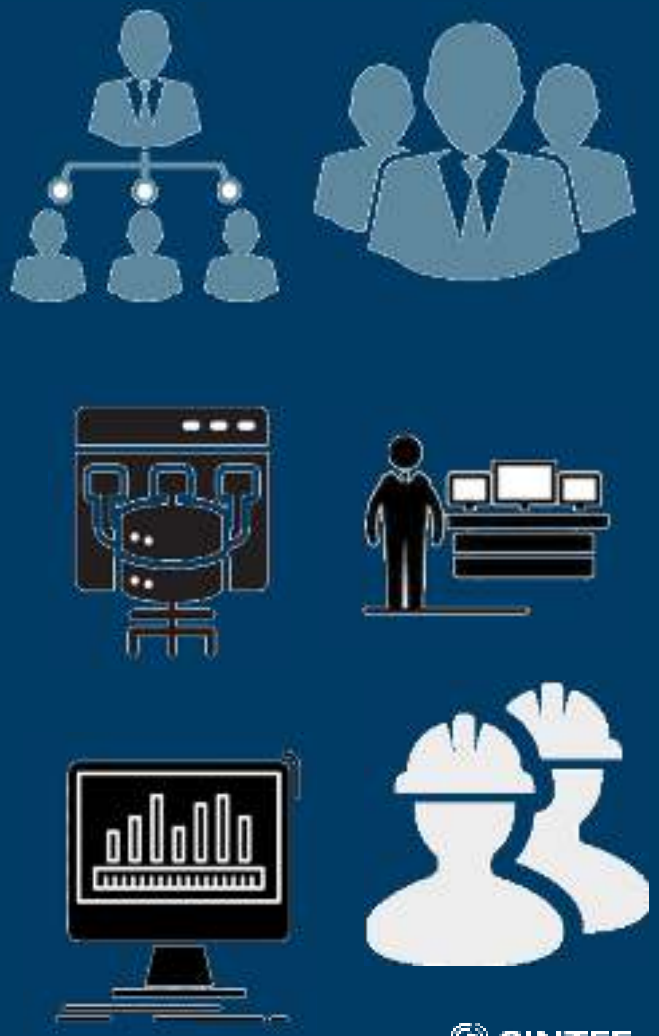
Nivå: prosjektgruppe
Kommunikasjon: Nettverk av forskjellige grupper av interessenter (relevante myndigheter, frivillige organisasjoner, teknologi leverandører, FoU-eksperter)
Konfidensialitetsnivå: lav/middels (i samsvar med sikkerhetsregler)

Nivå: Forskningsmiljøer og kritisk infrastruktur foreninger (utenfor VA-sektor)
Kommunikasjon: elektroniske medier, deltakelse i arrangementer
Konfidensialitetsnivå: ingen/lav

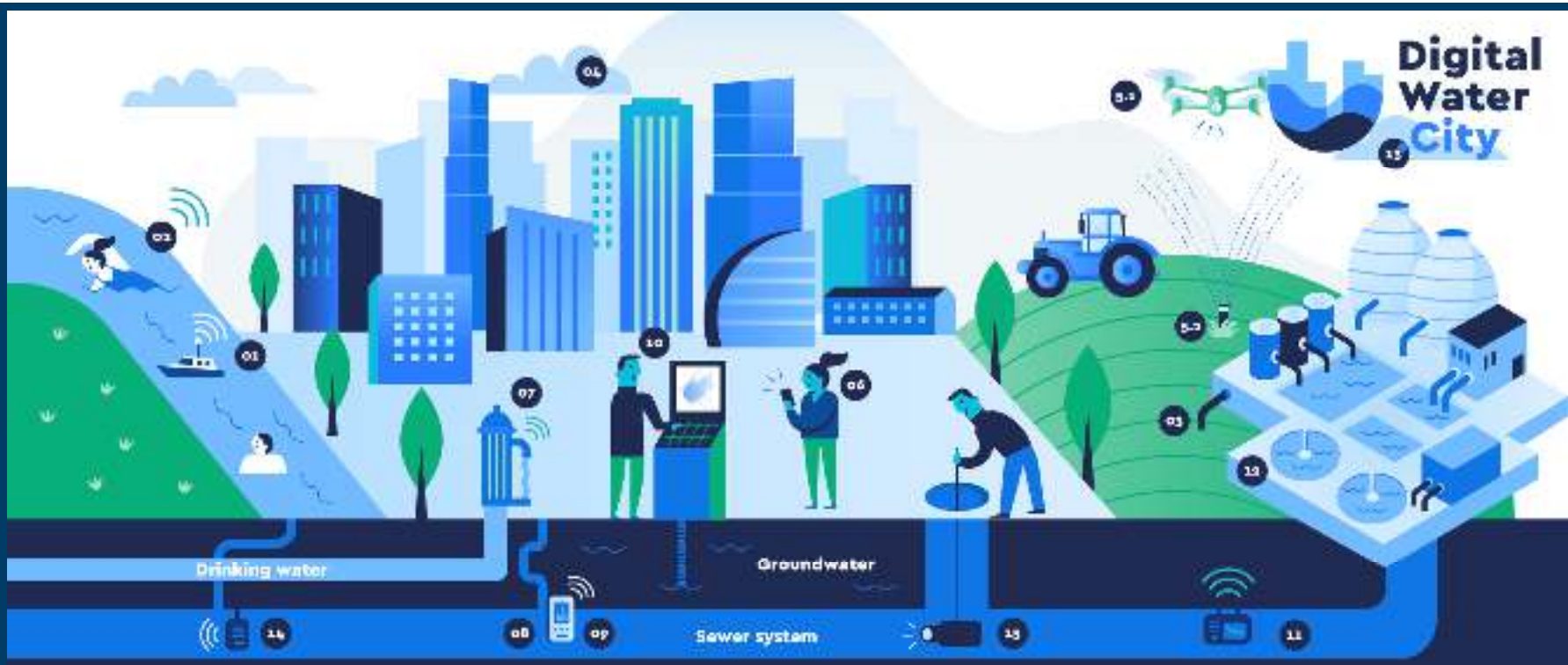
SINTEF
@seniorfrosk

Opplæringsaktiviteter

- STOP-IT læringsmateriell er tilpasset tre brukerprofiler
  - Beslutningstakere
  - Risikostyringsledere
  - Operatører
- Opplæring for beslutningstakere i juni 2019 (fysisk).
- Opplæring for risikostyringsledere i prosjektets "følge-vannverk" (FL) i november og desember 2019 (online).
- Individuelle webinarer rettet mot FL operatører på spesifikke verktøy nøye utvalgt av hver FL (video).



Digital Water City



15
digitale løsninger

5
byer

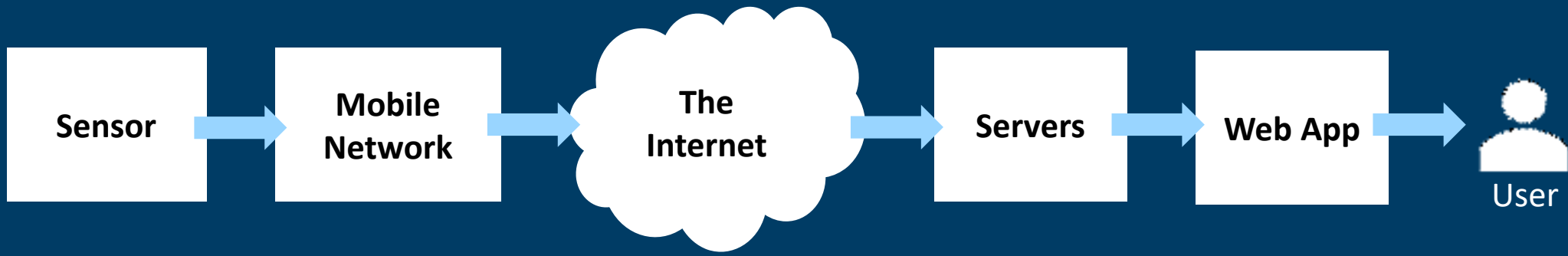
24
partnere

digital-water.city
digitalwater_eu

Angrep på IoT-baserte løsninger

- Tilgjengelige "fritt i lende"
- Typisk med dårligere sikkerhet (først på markedet, sikker maskinvare ikke tilgjengelig, …)
- Lav kostnad, potensielt høy konsekvens (sårbarheter kan ofte utnyttes i stor skale, f.eks. ved delte nøkler/passord)
- Mulig ny angrepsflate (hvis sensor f.eks. gir aksess til VPN)

Testet løsning

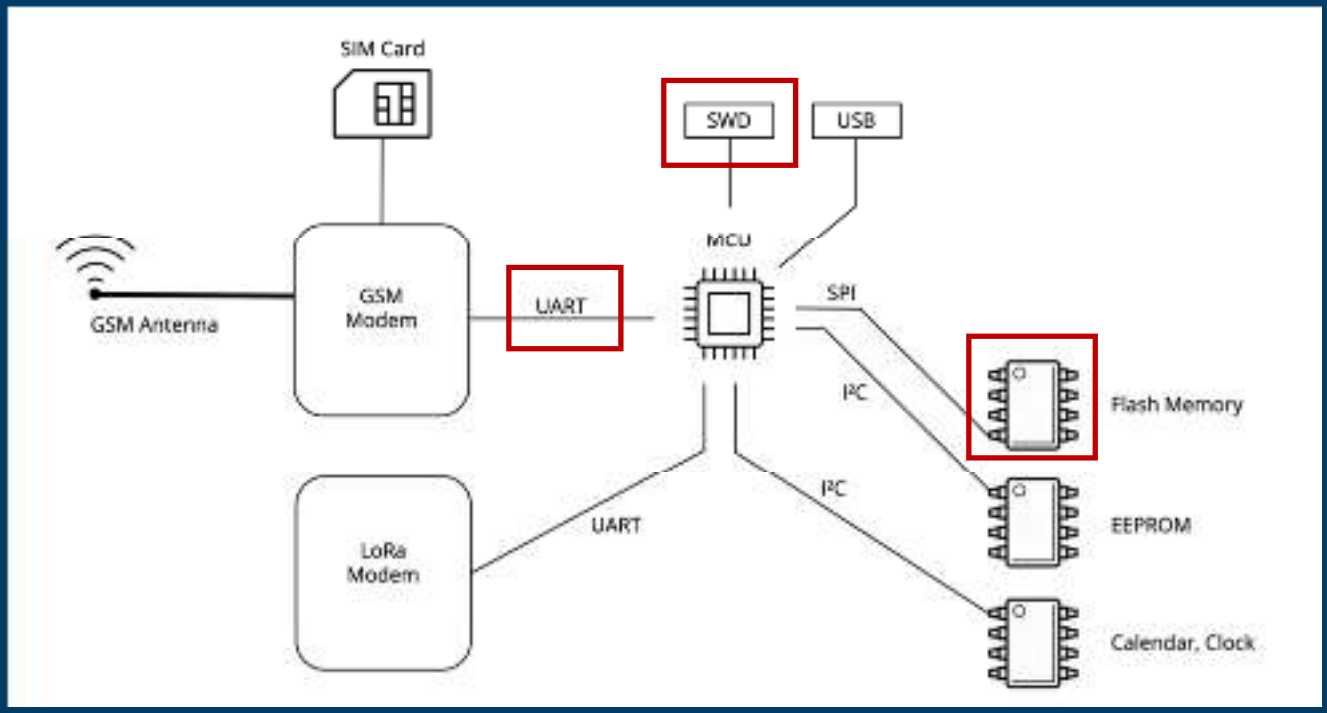


- Samler data fra miljøet og genererer varsler

Testmetodikk

- Vi ønsker å simulere et realistisk angrepsscenario
- Antagelse: en ekstern angriper har fått tilgang til /stjålet en installert enhet for å analysere den
- Svartboks-testing: ingen "inside-informasjon" fra produsenten er tilgjengelig

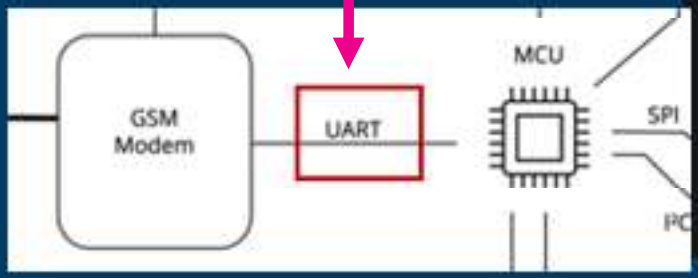
Maskinvareanalyse - oversikt



Lavthengende frukt

Universal asynchronous receiver-transmitter
Avlytting

Vi er her



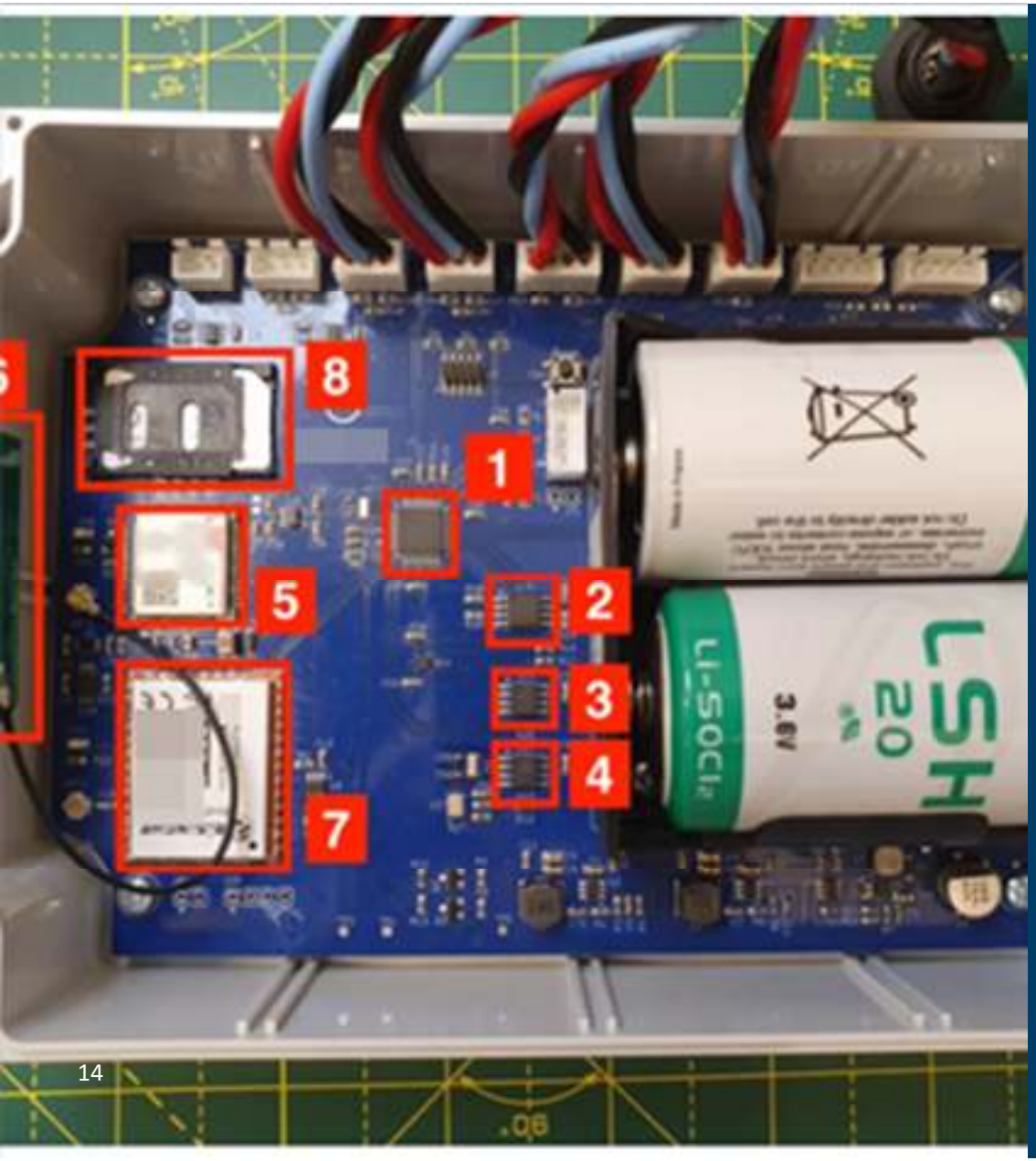

```
sudo comet --port /dev/ttyUSB4 --baud 38400 --port2 /dev/ttyUSB3 --baud2 38400
[*] port 1: /dev/ttyUSB4
[*] baudrate for port 1: 38400
[*] port 2: /dev/ttyUSB3
[*] baudrate for port 2: 38400
[*] Start listening on port 1...
[*] Start listening on port 2...
[<][2022-01-25 08:31:35.591117160 UTC] AT
[<][2022-01-25 08:31:36.102937463 UTC] AT
[>][2022-01-25 08:31:36.612037933 UTC] AT
[>][2022-01-25 08:31:36.612924115 UTC] OK
[<][2022-01-25 08:31:36.614810786 UTC] AT
[>][2022-01-25 08:31:37.038055484 UTC] RDY
...
[<][2022-01-25 08:32:02.503091138 UTC] AT+CIPSTATUS
[>][2022-01-25 08:32:02.506367586 UTC] STATE: IP INITIAL
[<][2022-01-25 08:32:02.519044767 UTC] AT+CSTT="[redacted]","","" ...
[>][2022-01-25 08:32:02.992367573 UTC] STATE: IP STATUS
[<][2022-01-25 08:32:04.006811292 UTC] AT+CIPSTART="UDP","[redacted]","[redacted]"
...
[>][2022-01-25 08:32:04.726390182 UTC] 2b4950442c34313a0004a30b014ff4d6010e87d7479c7aa6a8d582ed3c
6556007b81c062e1a0e97a5411a10a
[>][2022-01-25 08:32:04.736318108 UTC] 189d78fff90d0a
[<][2022-01-25 08:32:04.742702737 UTC] [redacted]c8cd74d6e5ccfa6df33f8b9e7131a68cd8
485077c0929bbd0234f5b2be41542b43495053454 e443d32350d0a
```


SINTEF

@seniorfrosk

En interessant observasjon

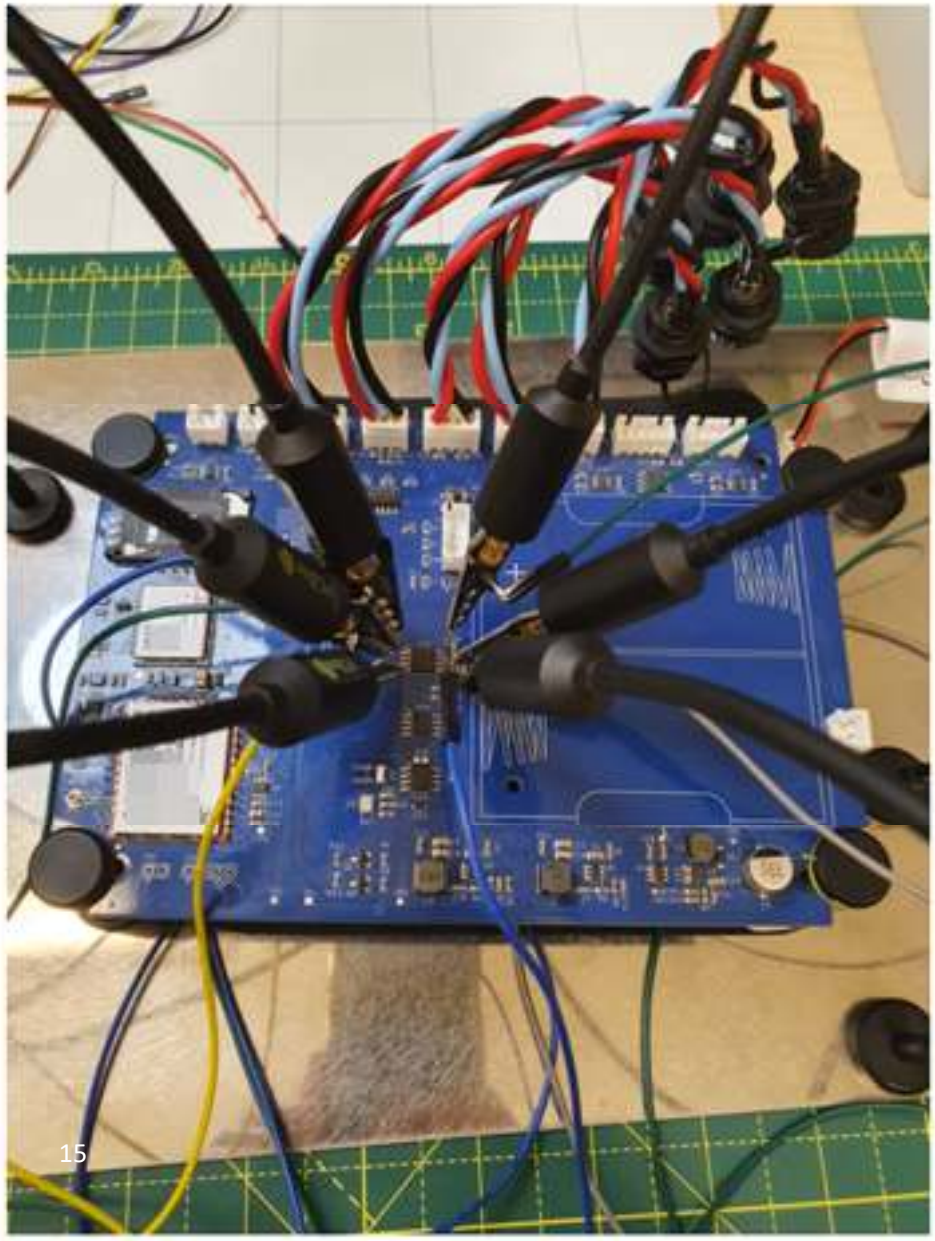
- Nyttelasten er alltid et multiplum av 16 byte
  - AES (intelligent gjetting)
- Vi oppdager samme nyttelast to ganger
  - ECB



Identifikasjon av komponenter

1. MCU
2. Flash Memory
3. EEPROM
4. Calendar, Clock IC
5. GSM Modem
6. GSM Antenna
7. LoRa Modem
8. SIM Card

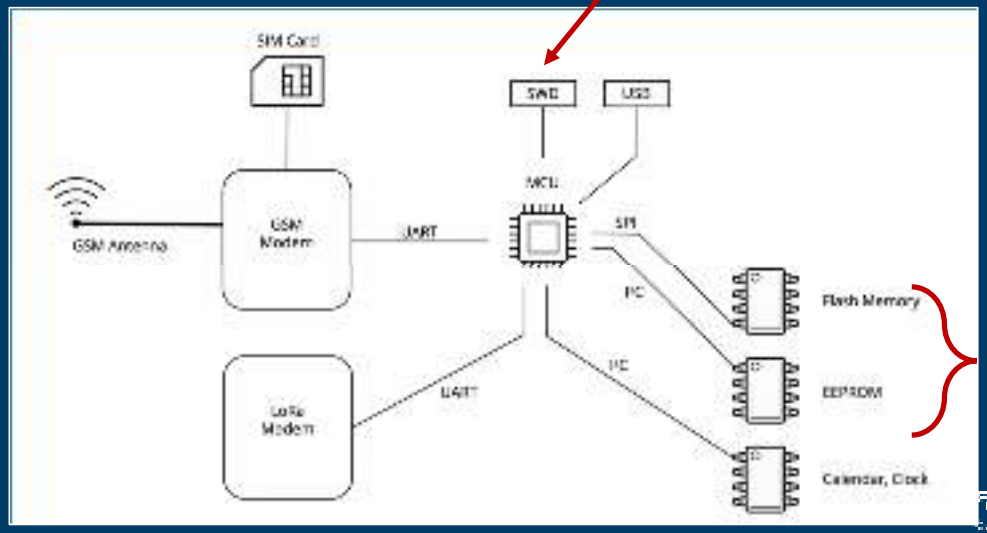
SINTEF
@seniorfrosk



Uthenting av firmware

- Firmware dumpes vha SWD-aksess
- Flash og EEPROM-innhold hentes ut ved å koble til og lese via SPI og I2C

Vi er her



Og her

SINTEF

@seniorfrosk

Hovedresultater

- En angriper kan gi seg ut for å være en enhet dersom han på et tidspunkt har fysisk tilgang til den
- En angriper kan utføre avspillingsangrep (replay attacks) og oversvømme serveren (fysisk tilgang ikke nødvendig)
- En angriper han IKKE reprodusere angrepet i stor skala (enheter må “hackes” individuelt, ettersom nøklene er unike)

Anbefalinger

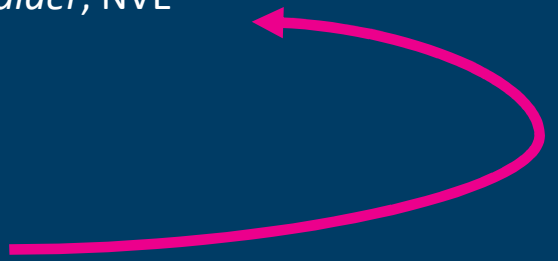
- Skru av debug-grensesnitt (SWD)
- Ikke lagre ukrypterte data på ekstern flash
- Bytt til en sikrere krypteringsmodus for AES
- https://www.sintef.no/contentassets/8fa5c7e3a81749b8952979000ee34c31/iot-security-checklist-v1.1.0.pdf

Leverandørkjede-sikkerhet – også for vannbransjen?

- Rapport for NVE
- Krav som små og mellomstore nettselskaper kan stille til sine leverandører

Metode

- Gjennomgang av tre tidligere rapporter fra NVE
  - Elisabeth Kirkebø, Mathias Ljøsne, *IKT-sikkerhet ved anskaffelser og tjenesteutsetting i energibransjen*, NVE Rapport 90:2018. [2]
  - Maren Maal, Katrine Krogedal og Arthur Gjengstø, *IKT-sikkerhet i anskaffelser og tjenesteutsetting i kraftbransjen - sjekkliste*, NVE- Rapport nr. 1/2020 [3]
  - Sigrid Haug Selnes, Sina Rebekka Moen, Siyang Emily Ji og Ove Njå, *Kraftbransjens leverandørkjeder – digital sikkerhet og sårbarhet i globaliseringens tidsalder*, NVE-Eksternrapport 18:2021 [5]
- Gjenvisitt hos veiledning for Kraftberedskapsforskriften
- Litteratursøk i nyere akademisk litteratur (etter 2021)
- Noen (veldig få) uformelle samtaler med aktører i bransjen



Må-krav

- Periodisk risikovurdering av leverandører
- Kartlegge hvordan leverandør kan bistå i en akutt situasjon
- Involver leverandører i øvelser

Må-krav (forts.)

- Servere plassert i EU/EØS (GDPR++)
- Servere som behandler kraftsensitiv informasjon må befinne seg i land som tilfredsstiller kravene til DKS klasse 2
- Ansatte med tilgang til sensitiv informasjon må befinne seg i EU/EØS
  - Vurder også nasjonalitet ("land vi har sikkerhetspolitisk samarbeid med)
- Nettselskapet må eie data i tjenesten som tilbys
  - Overføring av data og konfigurasjon ved terminering av kontrakt

Ytterligere krav

- Software Bill of Materials
- NSM grunnprinsipper eller tilsvarende
- VSA sjekkliste
- Prosess for håndtering av sårbarheter
- Redundans mellom underleverandører
  - NB: Hva er praktisk mulig? Hvor lang forsinkelse må man regne med?

Ytterligere krav (forts.)

- Oversikt over verdikjeder
- Automatisert monitorering av tjenester
- Sikker utvikling
- Herding av løsninger
  - NB: Kjører ting lokalt eller hos leverandør?
- Separasjon mellom kunder

Konklusjon og videre arbeid

- Leverandørkjedesikkerhet blir viktig også framover
  - Bør ha en ny runde med diskusjon med flere nettselskaper og leverandører
  - Og gjerne litt grundigere litteraturstudie

https://www.nve.no/nytt-fra-nve/nyheter-sikkerhet-og-energiforsyningsberedskap/krav-til-ikt-sikkerhet-for-kraftforsyningens-leverandoerer/

Spørsmål?

NORCICS SFI Norwegian Centre for Cybersecurity in Critical Sectors

SINTEF

Technology for a better society

https://infosec.sintef.no/

Martin.G.Jaatun@sintef.no

@seniorfrosk

@seniorfrosk@snabelen.no