Eemsgolaan 3
9727 DW Groningen
Postbus 1416
9701 BK Groningen

www.tno.nl

T +31 88 866 70 00
F +31 88 866 77 57

TNO-rapport

TNO 2019 R11252 | Eindrapport

Beveiliging watermanagement naar een hoger peil

Datum	1 oktober 2019
Auteur(s)	Dirk-Jan Brokken (TMX), Hans Besseling (TMX), Teake Bruinsma (Croonwolter&dros), Erik Bruinzeel (KPN), Eduard Hoekx (KPN), Auke Huistra (Applied Risk), Marcel Lange (Hunze en Aa's), Henri Maas (Brabantse Delta), John Bevers (Aa en Maas), Hiddo Hut (TNO), Arnoud de Jong (TNO), Edwin Matthijssen (TNO), Sjoerd-Jan Wiarda (TNO)
Exemplaarnummer	
Oplage	
Aantal pagina's	71 (incl. bijlagen)
Aantal bijlagen	3
Opdrachtgever	TKI HTSM
Projectnaam	Beveiliging watermanagement naar een hoger peil
Projectnummer	060.28469

Managementsamenvatting

Achtergrond
Door veranderingen in weersomstandigheden staan de Nederlandse waterschappen voor grote uitdagingen op gebieden als het beheer van grondwaterstanden en de bewaking van waterkwaliteit. Om deze uitdagingen het hoofd te bieden is een behoefte ontstaan om te onderzoeken of er vaker en op meer plekken metingen kunnen worden uitgevoerd. 'Internet of Things' (IoT) kan helpen om de metingen door te sturen naar de achterliggende infrastructuur van de waterschappen maar dat moet dan wel veilig gebeuren. Om te onderzoeken of IoT van toegevoegde waarde kan zijn voor de waterschappen hebben TMX, TNO, Croonwolter&dros, Applied Risk en KPN samen met de waterschappen Hunze en Aa's, Aa en Maas en Brabantse Delta het initiatief genomen tot het uitvoeren van een publiek-privaat onderzoeksproject binnen het Topsector programma HighTech Systemen & Materialen[1] (HTSM).

Onderzoeksvragen
In dit project is gekozen om gebruik te maken van de nieuwe IoT sensor-netwerktechnologie LoRaWAN®[2] en daar twee onderzoeksvragen voor te stellen:

1. Voldoet LoRaWAN aan de minimale set van eisen om te kunnen worden gebruikt in een nieuwe generatie van watertoepassingen?
2. Is het mogelijk om op een reproduceerbare manier aannemelijk te maken dat LoRaWAN veilig dan wel niet veilig genoeg is om te kunnen worden geadopteerd door de waterschappen in een nieuwe generatie van watertoepassingen?

Aanpak
In de eerste fase van het project is een set van minimale functionele eisen opgesteld in relatie tot twee use-cases die uitgevoerd moeten kunnen worden met deze sensornetwerk-technologie. In de tweede fase zijn zes proefopstellingen voor in het veld gebouwd op basis van prototype industriële sensoren. Deze veldopstellingen staan verspreid over drie locaties bij drie verschillende waterschappen in Nederland en zijn uitgeprobeerd aan de hand van functionele testscenario's. Daarnaast is een proefopstelling voor in een lab-omgeving gemaakt en voor deze proefopstelling zijn drie security testscenario's ontwikkeld.

Resultaten
De belangrijkste resultaten uit het project zijn:

1. LoRaWAN voldoet functioneel gezien aan de opgestelde set van minimale eisen om te kunnen worden gebruikt in toekomstige watertoepassingen.
2. Het oorspronkelijke idee van een geautomatiseerd security test-framework met daarin opgenomen allerlei security test-cases van meerdere beveiligingsbedrijven is niet haalbaar gebleken binnen de scope en het budget van dit project.
3. Binnen dit project zijn drie security testscenario's ontwikkeld en uitgeprobeerd op een privaat LoRaWAN sensornetwerk. Hieruit is onder andere gebleken dat de symmetrische LoRa Application Key, dit is een AES128-bit encryptie sleutel die wordt gebruikt om sessie sleutels af te

[1] Zie https://www.topsectoren.nl/
[2] LoRa® en LoRaWAN® zijn geregistreerde merknamen van de LoRa Alliance.

leiden, veilig moet worden opgeslagen. Aan de sensorkant zou dit bijvoorbeeld met een Secure Element in een sensor-node kunnen worden gedaan, afhankelijk van het beoogde dreigingsmodel.

Inhoudsopgave

1 Inleiding

1.1 Achtergrond

Door veranderingen in weersomstandigheden staan de Nederlandse waterschappen voor grote uitdagingen. “De jaarlijkse neerslagsom in Nederland is in de periode 1910-2017 gelijkmatig gestegen van 690 naar 874 millimeter. Dit is een toename van 27% in 108 jaar.”[3] Echter de ruimtelijke spreiding van de toename is niet gelijk over heel Nederland. Op sommige plaatsen worden intense regenbuien afgewisseld door langere periodes van droogte en dergelijke omstandigheden kunnen een grote impact hebben op de veiligheid en de economische bedrijvigheid in Nederland. Dit zou kunnen leiden tot een behoefte waarbij er veel vaker en op veel meer plekken metingen moeten worden uitgevoerd van water-gerelateerde omgevingsvariabelen. Informatietechnologie (IT) kan de waterschappen ondersteunen bij het uitvoeren van deze taken en dan met name de nieuwe mogelijkheden die met het ‘Internet of Things’[4] beschikbaar komen.

Internet of Things (IoT), letterlijk vertaald het Internet der Dingen, is een technologie waarbij apparaten zoals sensoren via netwerken worden verbonden aan applicaties om zo nieuwe toepassingen te kunnen ontwikkelen. Deze ontwikkeling creëert kansen en bedreigingen. Voor wat betreft de kansen kan IoT zorgen voor een toekomst waarin alles om ons heen wordt gemeten en aangestuurd en wordt toegepast in nieuwe applicaties die zo handig zijn dat we na verloop van tijd niet meer zonder kunnen. Voor wat betreft bedreigingen kunnen, met IT in het algemeen en met IoT in het bijzonder, cyber security en privacy risico’s ontstaan die tot schade (kosten) kunnen leiden.

In Nederland zijn meerdere IoT telecommunicatie-technologieën in opkomst: LoRaWAN[5], NarrowBand IoT[6] (NB-IoT), Sigfox[7] en LTE-M[8]. Alle varianten vallen in de zogenaamde Low Power Wide Area Network (LPWAN) categorie waarmee op efficiënte wijze vele sensoren en actuatoren over grote afstanden kunnen worden verbonden via sensornetwerken aan applicaties. Om te onderzoeken of IoT van toegevoegde waarde kan zijn voor de waterschappen hebben TMX, TNO, Croonwolter&dros, Applied Risk en KPN samen met de waterschappen Hunze en Aa’s, Aa en Maas en Brabantse Delta het initiatief genomen tot het starten van een onderzoeksproject. Dit betreft een publiek-privaat samenwerkingsproject dat wordt uitgevoerd binnen het programma van Topsectoren HighTech Systemen & Materialen (HTSM).

Dit document bevat de eindrapportage van het hierboven beschreven project.

[3] Zie https://www.clo.nl/indicatoren/nl0508-jaarlijkse-hoeveelheid-neerslag-in-nederland
[4] Zie https://en.wikipedia.org/wiki/Internet_of_things
[5] Zie https://nl.wikipedia.org/wiki/LoRaWAN
[6] Zie https://en.wikipedia.org/wiki/NarrowBand_IOT
[7] Zie Zie https://en.wikipedia.org/wiki/Sigfox
[8] Zie https://en.wikipedia.org/wiki/LTE-M

1.2 Doelstelling

Het doel van het samenwerkingsproject is het beantwoorden van de in het projectvoorstel beschreven onderzoeksvragen [1]. Deze twee onderzoeksvragen zijn door de projectpartners als volgt geformuleerd:

1. Voldoet LoRaWAN aan de minimale set van eisen om te kunnen worden gebruikt in een nieuwe generatie van watertoepassingen?

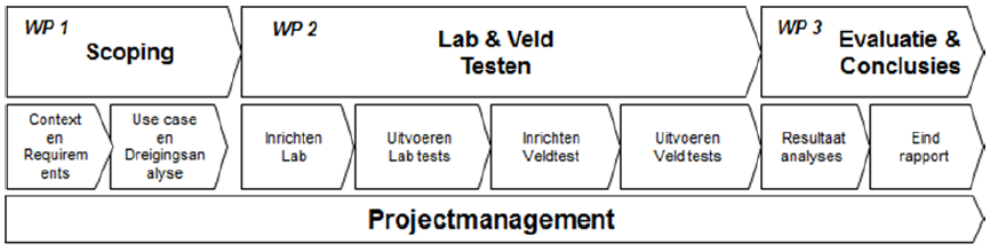
2. Is het mogelijk om op een reproduceerbare manier aannemelijk te maken dat LoRaWAN veilig dan wel niet veilig genoeg is om te kunnen worden geadopteerd door de waterschappen in een nieuwe generatie van watertoepassingen?

De eerste onderzoeksvraag gaat over *functionaliteit* in relatie tot de minimale set van eisen die gesteld worden door de waterschappen aan een moderne IoT watertoepassing. Denk hierbij bijvoorbeeld aan de ondersteuning voor twee-weg-communicatie voor het uitlezen van sensoren en het aansturen van actuatoren. De tweede onderzoeksvraag gaat over *veiligheid* (cyber security) van de sensorketen. Denk hierbij bijvoorbeeld aan de beveiliging van de sensormetingen en de beveiliging van de verschillende componenten en platformen in de sensorinfrastructuur.

Met deze doelstelling beogen de partners in het project een positieve bijdrage te leveren aan het verhogen van de cyberveiligheid van één van de belangrijkste kritieke infrastructuren in Nederland.

1.3 Aanpak

De gehanteerde aanpak bestaat globaal uit de volgende onderdelen (zie Figuur 1).



Figuur 1: Aanpak op hoofdlijnen

In werkpakket 1 vinden de activiteiten plaats waarin de scope, context en specifieke watertoepassing worden gekozen en vastgelegd ter voorbereiding van de testopstellingen.

In werkpakket 2 worden de testopstellingen ontwikkeld, zowel voor in het lab als voor in het veld. Voor deze testopstellingen worden prototype industriële sensoren ontwikkeld door de industriële partners Croon en TMX. De testopstellingen bestaan uit zowel een publiek als een privaat sensornetwerk waar deze prototype sensoren draadloos mee worden verbonden. Ook worden klantapplicaties (websites) ontwikkeld om de verstuurde sensorgegevens te ontvangen en visueel te

presenteren. De publieke versie van het sensornetwerk wordt gebaseerd op het LoRa netwerk van KPN. De private versie van het sensornetwerk wordt door TNO opgebouwd uit bestaande hardware- en software componenten zoals de “Kerlink Wirnet Station”[9] (gateways) en de software van LoRaServer[10]. Daarna wordt de private versie van het sensornetwerk als een proefopstelling bij Applied Risk in Amsterdam gebruikt voor het uitvoeren van security scenario’s. Voor de veldopstellingen bij de waterschappen worden zowel de publieke als de private sensornetwerken gebruikt voor het uitvoeren van functionele scenario’s.

In werkpakket 3 worden de onderzoeksresultaten van de testopstellingen geanalyseerd en wordt het onderzoek gedocumenteerd.

1.4 Scope

De volgende keuzes zijn gemaakt om de beschreven doelstelling te kunnen halen binnen de daarvoor beschikbaar gestelde hoeveelheid tijd.

- Het onderzoeksproject is ingekaderd tot alleen LoRaWAN. Bij deze technologie bestaat de mogelijkheid voor het uitrollen van een privaat netwerk vanwege de gebruikte licentievrije spectrumtechnologie en dit kan een interessant argument zijn voor de waterschappen.
- Het project richt zich vooral op de “End-to-End”[11] beveiliging van de ‘in-transit’[12] data in LoRaWAN door de sensorketen heen.
- Het project wordt uitgevoerd op basis van zowel een lab-opstelling als een veldopstelling waarin verschillende functionele- en security testscenario’s worden uitgevoerd. De reden hiervoor is dat de wens van de projectpartners om een nieuwe generatie van watertoepassingen mogelijk te maken erg ambitieus is. Voor die ambitie zou alleen een lab-opstelling niet overtuigend genoeg zijn.

[9] Zie https://www.kerlink.com/product/wirnet-station/
[10] Zie https://www.loraserver.io/
[11] Zie https://en.wikipedia.org/wiki/End-to-end_encryption
[12] Zie https://digitalguardian.com/blog/data-protection-data-in-transit-vs-data-at-rest

2 Context

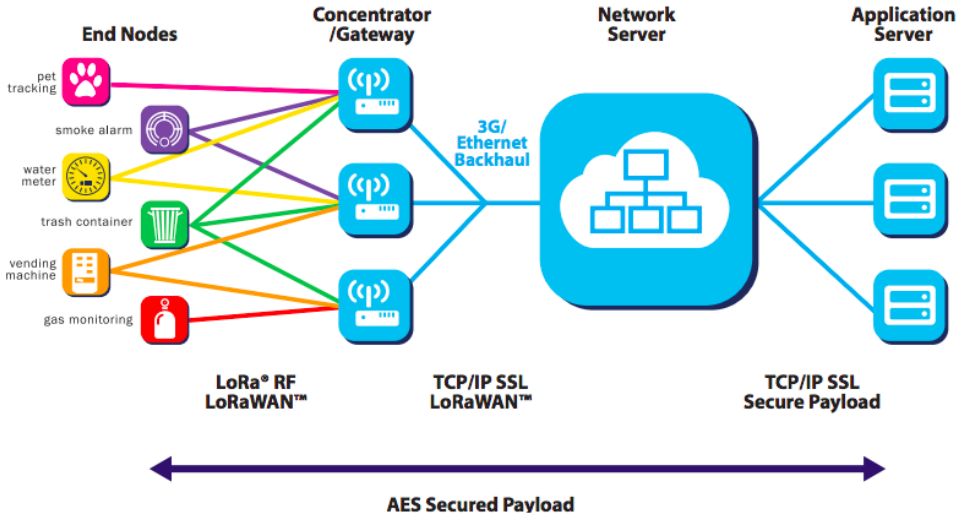
2.1 Wat is LoRaWAN

IoT in het algemeen gesproken gaat over het uitlezen en aansturen van “dingen” (objecten) en het verwerken van de resultaten daarvan in nieuwe toepassingen. De kernconcepten van IoT kunnen als volgt worden beschreven:

- ‘Sensing’ - Sensoren stellen ons in staat om informatie te verzamelen van objecten om ons heen. Denk bijvoorbeeld aan temperatuur, locatie, snelheid, vrije parkeerplaatsen en verder alle andere informatie die maar interessant kan zijn voor een bepaalde toepassing.
- ‘Controlling’ - IoT gaat niet alleen over het verzamelen van informatie maar ook over het aansturen van objecten zoals het openen van een klep of deur, het aan- of uitschakelen van objecten en verder alle andere aansturing die maar interessant kan zijn voor een bepaalde toepassing.
- ‘Software’ - Met vele objecten uit allerlei verschillende domeinen die uitgelezen of aangestuurd kunnen worden, kunnen nieuwe applicaties (software) worden bedacht en gemaakt waarmee innovatieve toepassingen mogelijk worden.
- ‘Network’ - Het verbinden van vele objecten via een telecommunicatie netwerk is nodig om de informatie van de objecten te kunnen versturen naar applicaties. De verwachting is dat deze applicaties nieuwe combinaties mogelijk zullen maken van toepassingen in verschillende domeinen.

LoRaWAN[13] is een IoT technologie en biedt interessante vernieuwingen op het gebied van spectrum, protocollen, beveiliging en kostprijs. De architectuur van een op LoRaWAN gebaseerd sensornetwerk ziet er typisch uit zoals weergegeven in Figuur 2.

[13] Zie https://nl.wikipedia.org/wiki/LoRaWAN

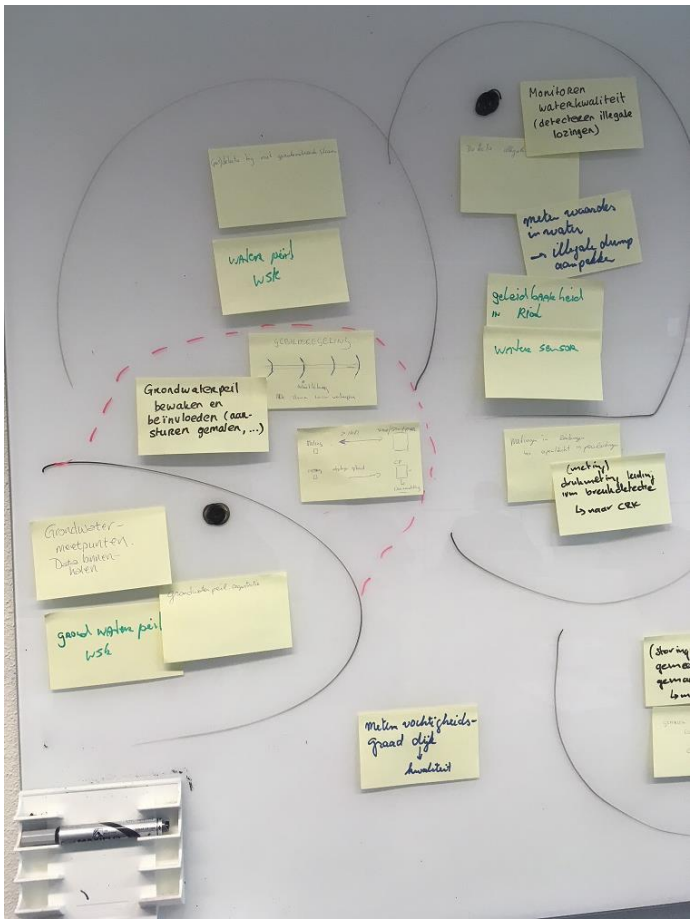


Figuur 2: LoRaWAN architectuur

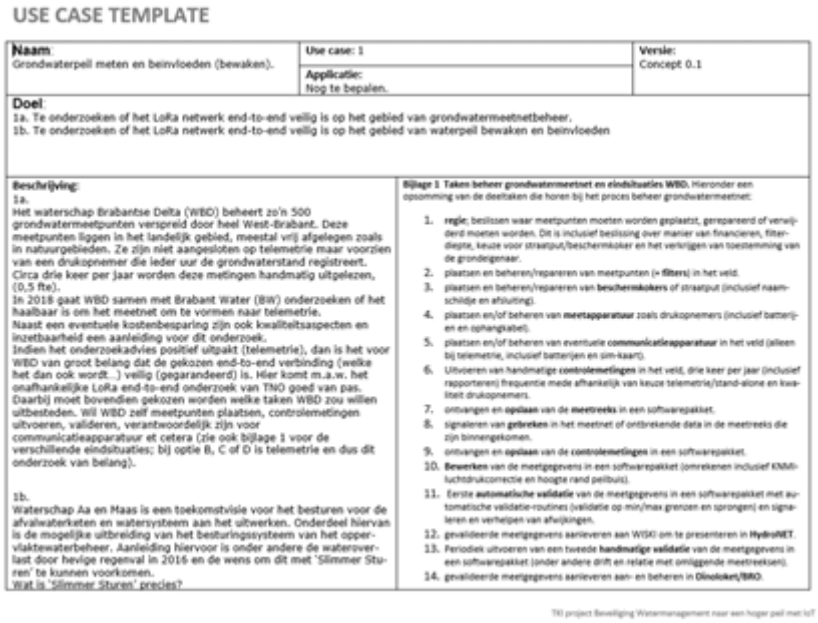
Aan de linkerkant staan allerlei sensoren weergegeven, ook wel End Nodes genoemd. Deze sensoren zijn een combinatie van een meet-element en een LoRa transceiver. Rechts daarvan weergegeven staan de Gateways die LoRa verkeer van de sensoren uit de lucht oppakken en doorsturen naar de Network Servers. De Network Servers hebben onder andere tot taak om ‘dubbelingen’ te detecteren en te filteren aangezien een bericht van een sensor door meerdere gateways kan worden opvangen. Aan de rechterkant staan de Application Servers waar de toepassingen op draaien die de sensordata ontvangen en verwerken. Bij de waterschappen zal dit in de meeste gevallen een ‘Supervisory Control and Data Acquisition ’ (SCADA) toepassing zijn.

2.2 Use-cases

In een brainstorm sessie met de projectdeelnemers is nagedacht over welke use-cases interessant zijn voor de waterschappen (zie Figuur 3). De enige beperking op de ideeën is dat de sensoren gekocht moeten kunnen worden en moeten passen in het projectbudget.



Figuur 3: Brainstorm sessie over Use-cases



USE CASE TEMPLATE

Naam: Grondwaterpeil meten en beinvloeden (bewaken).	**Use case:** 1 **Applicatie:** Nog te bepalen.	**Versie:** Concept 0.1

Doel:
1a. Te onderzoeken of het LoRa netwerk end-to-end veilig is op het gebied van grondwatermeetnetbeheer.
1b. Te onderzoeken of het LoRa netwerk end-to-end veilig is op het gebied van waterpeil bewaken en beinvloeden

Beschrijving:
1a.
Het waterschap Brabantse Delta (WBD) beheert zo'n 500 grondwatermeetpunten verspreid door heel West-Brabant. Deze meetpunten liggen in het landelijk gebied, meestal vrij afgelegen zoals in natuurgebieden. Ze zijn niet aangesloten op telemetrie maar voorzien van een drukopnemer die ieder uur de grondwaterstand registreert. Circa drie keer per jaar worden deze metingen handmatig uitgelezen, (0,5 fte).
In 2018 gaat WBD samen met Brabant Water (BW) onderzoeken of het haalbaar is om het meetnet om te vormen naar telemetrie.
Naast een eventuele kostenbesparing zijn ook kwaliteitsaspecten en inzetbaarheid een aanleiding voor dit onderzoek.
Indien het onderzoekadvies positief uitpakt (telemetrie), dan is het voor WBD van groot belang dat de gekozen end-to-end verbinding (welke het dan ook wordt...) veilig (gegarandeerd) is. Hier komt m.a.w. het onafhankelijke LoRa end-to-end onderzoek van TNO goed van pas. Daarbij moet bovendien gekozen worden welke taken WBD zou willen uitbesteden. Wil WBD zelf meetpunten plaatsen, controlemetingen uitvoeren, valideren, verantwoordelijk zijn voor communicatieapparatuur et cetera (zie ook bijlage 1 voor de verschillende eindsituaties; bij optie B, C of D is telemetrie en dus dit onderzoek van belang).

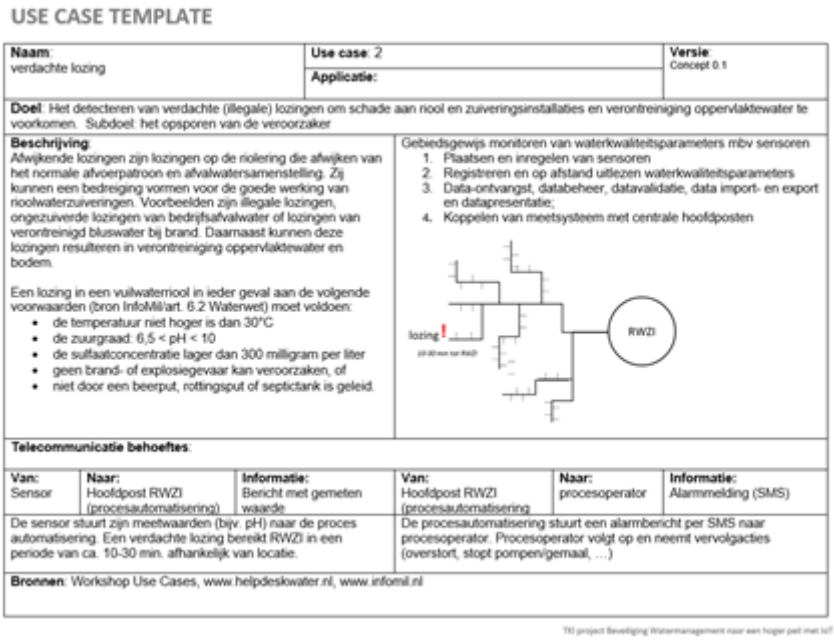
1b.
Waterschap Aa en Maas is een toekomstvisie voor het besturen voor de afvalwaterketen en watersysteem aan het uitwerken. Onderdeel hiervan is de mogelijke uitbreiding van het besturingssysteem van het opper-vlaktewaterbeheer. Aanleiding hiervoor is onder andere de waterover-last door hevige regenval in 2016 en de wens om dit met 'Slimmer Stu-ren' te kunnen voorkomen.
Wat is 'Slimmer Sturen' precies?

Bijlage 1 Taken beheer grondwatermeetnet en eindsituaties WBD. Hieronder een opsomming van de deeltaken die horen bij het proces beheer grondwatermeetnet:

1. **regie**, beslissen waar meetpunten moeten worden geplaatst, gerepareerd of verwijderd moeten worden. Dit is inclusief beslissing over manier van financieren, filterdiepte, keuze voor straatput/beschermkoker en het verkrijgen van toestemming van de grondeigenaar.
2. plaatsen en beheren/repareren van meetpunten (= **filters**) in het veld.
3. plaatsen en beheren/repareren van **beschermkokers** of straatput (inclusief naamschildje en afsluiting).
4. plaatsen en/of beheren van **meetapparatuur** zoals drukopnemers (inclusief batterij- en en ophangkabel).
5. plaatsen en/of beheren van eventuele **communicatieapparatuur** in het veld (alleen bij telemetrie, inclusief batterijen en sim-kaart).
6. Uitvoeren van handmatige **controlemetingen** in het veld, drie keer per jaar (inclusief rapporteren) frequentie mede afhankelijk van keuze telemetrie/stand-alone en kwaliteit drukopnemers.
7. ontvangen en **opslaan** van de **meetreeks** in een softwarepakket.
8. signaleren van **gebreken** in het meetnet of ontbrekende data in de meetreeks die zijn binnengekomen.
9. ontvangen en **opslaan** van de **controlemetingen** in een softwarepakket.
10. **Bewerken** van de meetgegevens in een softwarepakket (omrekenen inclusief KNMI-luchtdrukcorrectie en hoogte rand peilbuis).
11. Eerste **automatische validatie** van de meetgegevens in een softwarepakket met automatische validatie-routines (validatie op min/max grenzen en sprongen) en signaleren en verhelpen van afwijkingen.
12. gevalideerde meetgegevens aanleveren aan WISKI om te presenteren in **HydroNET**.
13. Periodiek uitvoeren van een tweede **handmatige validatie** van de meetgegevens in een softwarepakket (onder andere drift en relatie met omliggende meetreeksen).
14. gevalideerde meetgegevens aanleveren aan- en beheren in **Dinoloket/BRO**.

TKI project Beveiliging Watermanagement naar een hoger peil met IoT

Figuur 4: Use-case-1 Grondwaterpeil meten



USE CASE TEMPLATE

Naam: verdachte lozing	**Use case**: 2 **Applicatie:**	**Versie**: Concept 0.1

Doel: Het detecteren van verdachte (illegale) lozingen om schade aan riool en zuiveringsinstallaties en verontreiniging oppervlaktewater te voorkomen. Subdoel: het opsporen van de veroorzaker

Beschrijving:
Afwijkende lozingen zijn lozingen op de riolering die afwijken van het normale afvoerpatroon en afvalwatersamenstelling. Zij kunnen een bedreiging vormen voor de goede werking van rioolwaterzuiveringen. Voorbeelden zijn illegale lozingen, ongezuiverde lozingen van bedrijfsafvalwater of lozingen van verontreinigd bluswater bij brand. Daarnaast kunnen deze lozingen resulteren in verontreiniging oppervlaktewater en bodem.

Een lozing in een vuilwaterriool in ieder geval aan de volgende voorwaarden (bron InfoMil/art. 6.2 Waterwet) moet voldoen:
- de temperatuur niet hoger is dan 30°C
- de zuurgraad: 6,5 < pH < 10
- de sulfaatconcentratie lager dan 300 milligram per liter
- geen brand- of explosiegevaar kan veroorzaken, of
- niet door een beerput, rottingsput of septictank is geleid.

Gebiedsgewijs monitoren van waterkwaliteitsparameters mbv sensoren
1. Plaatsen en inregelen van sensoren
2. Registreren en op afstand uitlezen waterkwaliteitsparameters
3. Data-ontvangst, databeheer, datavalidatie, data import- en export en datapresentatie;
4. Koppelen van meetsysteem met centrale hoofdposten

Telecommunicatie behoeftes:

Van:	Naar:	Informatie:	Van:	Naar:	Informatie:
Sensor	Hoofdpost RWZI (procesautomatisering)	Bericht met gemeten waarde	Hoofdpost RWZI (procesautomatisering	procesoperator	Alarmmelding (SMS)
De sensor stuurt zijn meetwaarden (bijv. pH) naar de proces automatisering. Een verdachte lozing bereikt RWZI in een periode van ca. 10-30 min. afhankelijk van locatie.			De procesautomatisering stuurt een alarmbericht per SMS naar procesoperator. Procesoperator volgt op en neemt vervolgacties (overstort, stopt pompen/gemaal, …)		

Bronnen: Workshop Use Cases, www.helpdeskwater.nl, www.infomil.nl

Figuur 5: Use-case-2: Waterkwaliteit meten (verdachte lozing)

Uiteindelijk hebben de waterschappen gekozen voor het willen kunnen meten van een waterpeil (zie Figuur 4) en het meten van een parameter van de kwaliteit van het water (zie Figuur 5) zoals bijvoorbeeld ammonium, nitraat, fosfaat, zuurgraad, zuurstof of temperatuur.

2.3 Requirements

In een brainstorm sessie met de waterschappen en de industriële partijen CroonWolter&Dros en TMX is nagedacht over de minimale set van eisen voor de gekozen use-cases. Met andere woorden: waar moet een oplossing aan voldoen om bruikbaar te zijn voor de waterschappen. Hiermee worden toepassingen voor zowel de waterkwantiteit als waterkwaliteit meegenomen in dit onderzoek. Het doel is vooral om inzichtelijk te krijgen onder welke voorwaarden de use-cases grofweg gebruikt moeten kunnen worden in de praktijk.

Voor de formulering en de inhoud van de eisen hebben we de volgende spelregels afgesproken:
- De eisen moeten uniek identificeerbaar zijn.
- De eisen moeten technologie-onafhankelijk worden geformuleerd (geen vendors of producten).
- De eisen moeten traceerbaar zijn naar een betrokken stakeholder of eigenaar.
- De eisen moeten op functioneel niveau worden geformuleerd.

ID1
De communicatietechnologie moet 'tweeweg' verkeer ondersteunen.
Partij: Waterschap en TMX
Commentaar:

Onderstations en dataloggers communiceren via tweeweg communicatie. Tweeweg communicatie is noodzakelijk om de volgende noodzakelijke functionaliteiten te kunnen ondersteunen:

- Vanuit het device worden registraties naar de hoofdpost verzonden; bijvoorbeeld een grondwaterpeil. Als de hoofdpost één of meerdere registraties mist dan dienen deze opnieuw opgevraagd te kunnen worden door de hoofdpost bij de datalogger. Dit synchroniseren gebeurd standaard door telemetrieapparatuur na het herstellen van een verbinding. De compleetheid van een datareeks wordt door gebruikers gezien als een kwaliteitskenmerk.
- Het op afstand kunnen aanpassen van instellingen in het apparaat. Dit is noodzakelijk om bijvoorbeeld communicatie-instellingen of een registratie-interval aan te kunnen passen.
- De mogelijkheid om de firmware van het betreffende apparaat op afstand te kunnen updaten. Deze mogelijkheid wordt vaak aangeduid als Firmware Over The Air, kortweg FOTA. Zie ID-6 voor een nadere uitleg.

ID2
Een sensor moet minimaal eens per uur een meting kunnen versturen naar een hoofdpost.
Partij: Waterschap
Commentaar:

ID3
Sensoren moeten geschikt zijn om datgene te meten wat in de use-case is afgesproken.
Partij: Waterschap
Commentaar:

ID4
Backoffice moet sensordata kunnen opslaan van minimaal één jaar van alle sensoren.
Partij: Waterschap
Commentaar:

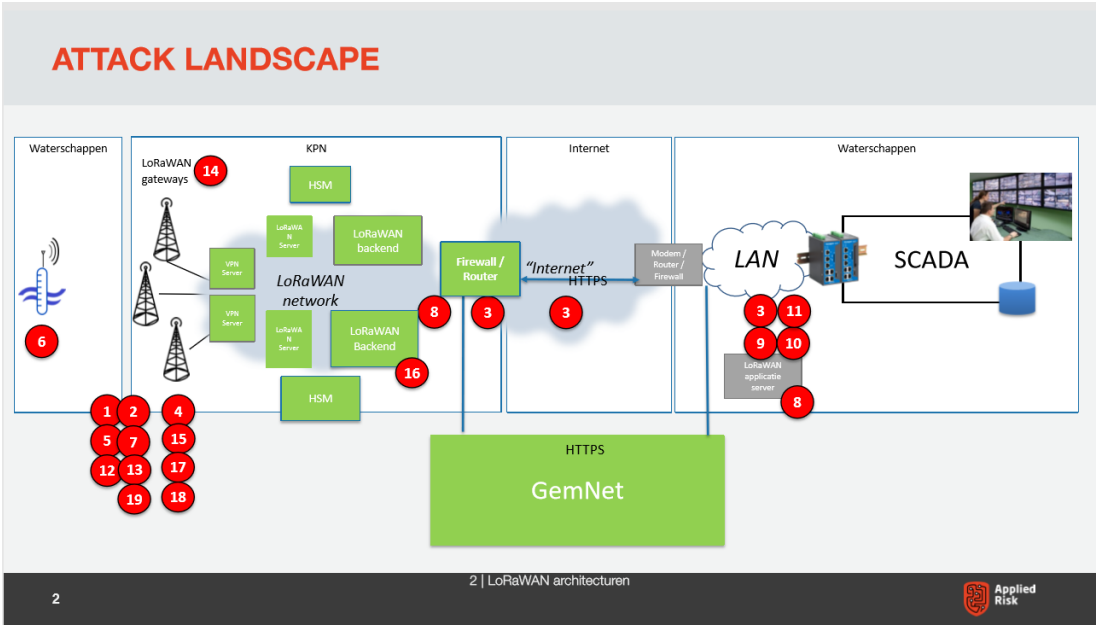
ID5
Telecom infrastructuur moet 90% beschikbaar zijn op jaarbasis.
Partij: Waterschap
Commentaar:

ID6
Firmware van sensoren moet op afstand kunnen worden bijgewerkt.
Partij: TMX
Commentaar:
Moderne onderstations en dataloggers beschikken over de mogelijkheid om de firmware van het betreffende apparaat op afstand te kunnen updaten. Deze mogelijkheid wordt aangeduid als Firmware Over The Air, kortweg FOTA. Vanuit security oogpunt is het noodzakelijk om over FOTA te beschikken. Zo kan bijvoorbeeld een fout die na installatie van een apparaat in het veld ontdekt wordt, achteraf en op afstand opgelost worden.

ID7
Batterij van IoT-apparatuur moet lang mee gaan (5 tot 10 jaar).
Partij: TMX
Commentaar:
Batterijgevoede IoT-apparatuur kenmerkt zich door een hele lage Total Cost of Ownership (TCO). Om deze lage TCO te bereiken zal de batterij lang mee moeten gaan; voor een LoRa-device typisch 5 tot 10 jaar. Het moeten vervangen van de batterij in het veld is sterk kostenverhogend. De kosten (manuren / reiskosten / aanschafkosten) voor een batterijvervanging zullen bij IoT-apparatuur in veel gevallen hoger zijn dan de aanschafprijs van het betreffende apparaat.

2.4 Risicoanalyse

In een brainstorm sessie met Applied Risk en KPN Security is naar aanleiding van een paper “LoRaWAN: Vulnerability Analysis and Practical Expoitation” van Yang Xueying (TU Delft, 2017) [3] nagedacht over mogelijke aanvalsscenario’s en op welke plekken in de infrastructuur van een sensorketen deze zouden kunnen worden uitgevoerd (zie Figuur 6).



Figuur 6: Mogelijke aanvalsscenario's

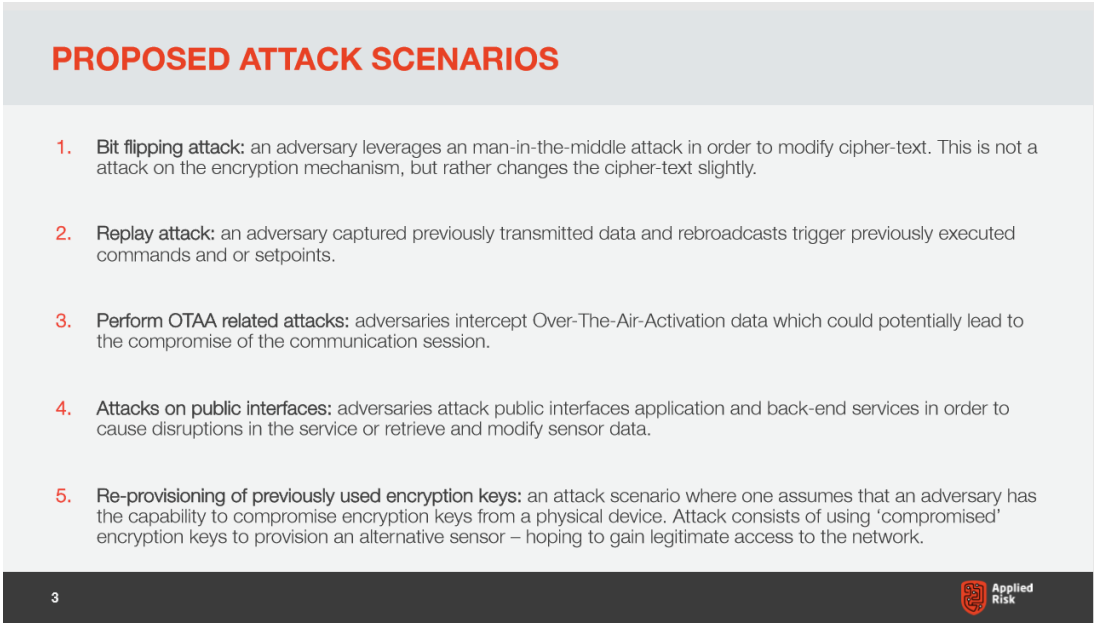
Daarna is bekeken welke negatieve effecten (impact) dergelijke aanvallen zouden kunnen hebben op een use-case (zie Figuur 7).

nr	scenario	effect	kwetsbaarheid	categorie	uitvoerbaarheid
1	Replay aanval met malicious device	Sensor kan geen berichten meer versturen	protocol	Beschikbaarheid	makkelijk
2	Afluisteraanval	Sensorwaarde worden afgeluisterd	protocol	Vertrouwelijkheid	moeilijk
3	Bit-flipping aanval	Meetwaarden kunnen aangepast	protocol	Integriteit	makkelijk
4	Spoof met malicious gateway	Meting van een sensor wordt tegengehouden	protocol	Beschikbaarheid	makkelijk
5	Replay aanval via join-procedure	Verbinding tussen een sensor en een gateway wordt verstoord	protocol	Beschikbaarheid	makkelijk
6	Encryptiesleutels worden uit een device gehaald en hergebruikt	Aanvaller kan correct ondertekende en vercijferde berichten versturen	device	Integriteit & vertrouwelijkheid	moeilijk
7	Signal-jammer	Verbinding tussen een sensor en een gateway wordt verstoord	spectrum	Beschikbaarheid	makkelijk
8	Aanvaller heeft toegang tot een LoRaWAN backend systeem	Meetwaarden kunnen verwijderd	platform access	Beschikbaarheid	makkelijk
9	DDoS aanval	Sensoren kunnen geen meetwaarden afleveren op server	network	Beschikbaarheid	makkelijk
10	Aanval op de LoRaWAN applicatie server	Beschikbaarheid server verstoord, software aangepast, meetwaarden achterhaald	platform	Beschikbaarheid, Integriteit, vertrouwelijkheid	moeilijk

Figuur 7: Inschatting effect en uitvoerbaarheid

Ook over de uitvoerbaarheid van een aanval is nagedacht, met andere woorden is een aanval makkelijk of moeilijk te ontwikkelen en makkelijk of moeilijk uit te voeren. Niet alleen om in te schatten wat een aanvaller daadwerkelijk zou kunnen gaan proberen in Nederland. Maar ook omdat Applied Risk in dit onderzoek enkele van deze aanvallen gaat implementeren en gaat uitproberen op een proefopstelling in hun lab omgeving in Amsterdam.

Uiteindelijk is een short-list gemaakt van vijf scenario's (in willekeurige volgorde) die voor het project interessant zijn én die binnen het beperkte budget ontwikkeld en uitgeprobeerd kunnen worden.



Figuur 8: Voorgestelde scenario's

2.5 Methodiek

De gehanteerde onderzoeksmethodiek valt uiteen in twee delen:

Functionaliteit
Voor dit samenwerkingsproject onderzoeken we of LoRaWAN goed werkt met betrekking tot use-cases die interessant zijn voor de waterschappen. De voor dit project gekozen methodiek om dat aannemelijk te maken, is gebaseerd op contra-metingen. Door op locaties in het veld bij de waterschappen met LoRa een parameter te meten die ook door de waterschappen zelf gemeten wordt, kan onderzocht worden of de opstellingen functioneel gezien vergelijkbaar zijn. Uiteraard zullen log-frequentie en het communicatie-interval geoptimaliseerd worden voor Low Power toepassingen waar LoRa voor bedoeld is. Omdat er een sensor voor zowel waterkwaliteit als waterkwantiteit wordt gekozen, waarbij de waterkwantiteitssensor het waterniveau meet en de waterkwaliteitssensor een fysische parameter, wordt de werking voor meerdere toepassingen aangetoond. De deelnemende waterschappen wordt gevraagd om de datasets van hun contra-metingen van de betreffende parameters in de vorm van tijdreeksen ter beschikking te stellen voor dit project zodat het vergelijk gemaakt kan worden.

Veiligheid
De voor dit project gekozen security methodiek is het uitproberen van enkele ‘hack’ aanvallen naar aanleiding van het paper van Yang Xueying [3]. Industrieel cyber security bedrijf Applied Risk gaat een aantal aanvallen implementeren en kijken hoe de proefopstelling daarmee omgaat. Het idee is dat als één van deze scenario’s een onacceptabel effect heeft op een use-case, dat dan de specifieke implementatie van de proefopstelling niet goed genoeg is voor de Nederlandse kritieke infrastructuur. Andersom geredeneerd, namelijk als blijkt dat de proefopstelling wel bestand is tegen alle uitgeprobeerde aanvallen, is een conclusie lastiger te duiden. Bewijzen dat een opstelling niet goed genoeg is, is relatief simpel aan te tonen door het uitvoeren van een succesvolle aanval. Echter bewijzen dat een opstelling 100% veilig is, is praktisch onmogelijk.

Zie Bijlage A voor meer achtergrondinformatie over deze aanpak in relatie tot een Nationaal Cybersecurity Testbed.

3 Gebruikte proefopstellingen

3.1 Overzicht locaties

Er zijn in totaal zes veldopstellingen geplaatst bij drie verschillende waterschappen. Per locatie zijn twee opstellingen neergezet:

- Eén opstelling voor het meten van het waterniveau (waterkwantiteit).
- Eén opstelling voor het meten van een fysische parameter (waterkwaliteit). Dit wordt gedaan door het meten van de temperatuur of de pH-waarde.

Waterschap	Locatienaam	Adres
Hunze en Aa's	RWZI Scheve Klap	Heemweg 20-21, Woldendorp
Brabantse Delta	RWZI Chaam	Elsakkerpad 15, Chaam
Aa en Maas	RWZI Dinther	Hazelbergsestraat 5, Heeswijk Dinther

Tabel 1: Overzicht van de locaties

De waterschappen hebben hiervoor de volgende locaties ter beschikking gesteld (zie Figuur 9).

Figuur 9: Locaties van de veldopstellingen

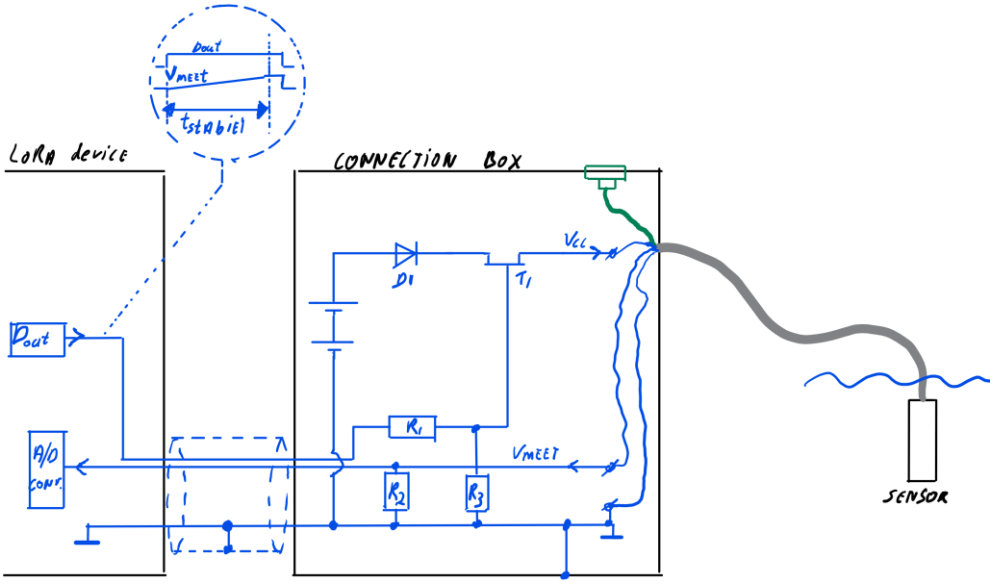
3.2 Connection Box

Voor het project is een Connection Box door TMX ontwikkeld. Deze is nodig om de sensoren te kunnen koppelen aan de LoRa nodes. De Connection Box zorgt voor

voeding van de sensor en signaalconditionering zodat de sensordata op de analoge ingang van de LoRa-logger aangesloten kan worden. Om de installatie eenvoudig te houden is de LoRa-logger van CroonWolter&Dros ook in de Connection Box kast gemonteerd. Zie Figuur 10 voor een close-up van de Connection Box.

Figuur 10: Close-up van Connection Box

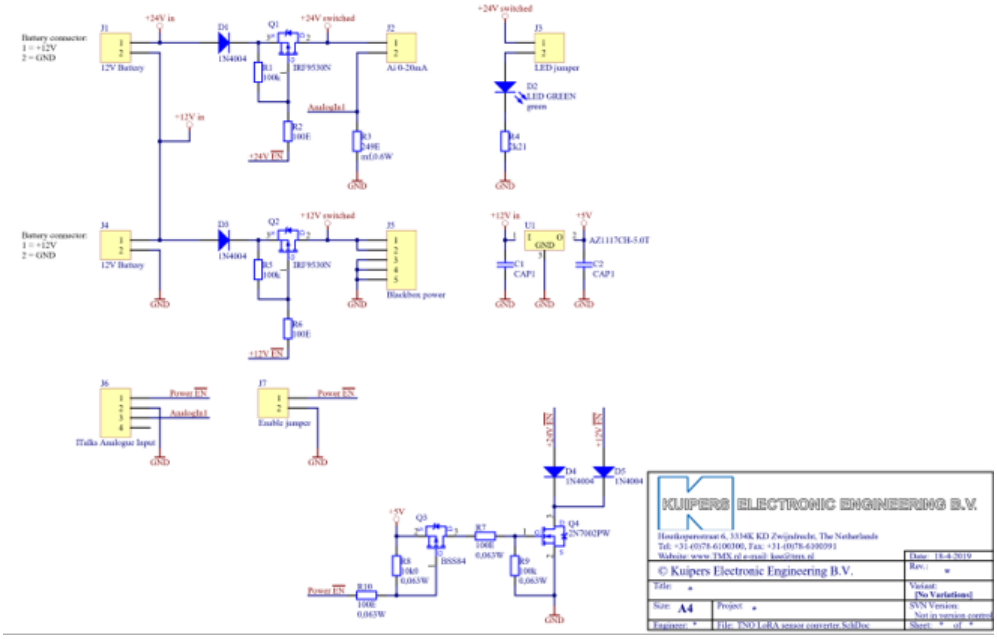
Onderstaande schets geeft weer hoe een waterniveausensor wordt aangesloten op de LoRa-loggers.



Figuur 11: Principeschema van Connection box, LoRa-logger en waterniveau sensor

De batterijen in de Connection box hebben voldoende capaciteit om de sensor tenminste drie maanden van spanning te kunnen voorzien. Om de capaciteit (en formaat/prijs) van de batterijen acceptabel te houden, wordt de voeding van de sensor door middel van een digitale uitgang uit de logger in- en uitgeschakeld. De programmering van de LoRa-logger zorgt ervoor dat de digitale uitgang van de logger enige tijd voor het ‘samplen’ van de analoge ingang actief wordt. Als de sample gemeten is dan wordt de digitale uitgang gelijk weer laag om zoveel mogelijk energie te sparen.

Bovengenoemde principeschema voor de Connection Box tussen de LoRa-logger en de waterniveausensor is omgezet naar een definitieve uitvoering zoals hieronder weergegeven.



Figuur 12 Schema interfaceprint connection box

Figuur 13: Sensor testomgeving

3.3 Sensoren

De toegepaste LoRa loggers zijn gebaseerd op de ITALKS MCS 1608[14] en beschikken over één analoge ingang (0 - 5 Volt) voor het aansluiten van een sensor. Omdat de LoRa-logger batterij-gevoed is, moet de sensor ook zijn voeding uit een batterij krijgen. Om batterij te besparen kan de logger via een interface print in de Connection Box de voeding van de sensor uitschakelen als deze niet nodig is. De programmering van de LoRa logger is hiervoor aangepast.

De eisen aan de sensoren zijn:

- 4 – 20 mA uitgang
- 12 – 24 Volt dc voedingsspanning (zo laag mogelijk)
- zo laag mogelijke stroomopname
- zo kort mogelijke opwarmtijd na inschakeling
- eenvoudig te ijken c.q. controleren
- waterdicht (IP67 of beter)
- afstand sensor tot Connection Box zo kort mogelijk (niet langer dan 10 meter)

Uit een groot scala aan mogelijke sensoren zijn twee sensoren geselecteerd. Om een verifieerbaar resultaat te krijgen, zijn er sensoren geselecteerd welke een fysische parameter meten die op de betreffende locatie ook op de RWZI door het Waterschap gemeten wordt. De gemeten waarden kunnen op deze wijze achteraf

[14] Zie https://www.mcs-nl.com/producten/italks-mcs-1608-full-lora-sensor

vergeleken worden met de metingen van het betreffende Waterschap zodat bewezen kan worden dat de opstellingen in de praktijk correct functioneren.

Er is geïnventariseerd bij de drie waterschappen welke parameters op de RWZI's gemeten worden en hieruit zijn de volgende parameters en sensoren geselecteerd.

Parameter	Parameter aanwezig op locatie		
	WSHA - Scheve Klap	WSBD - Chaam	WSAM - Dinther
NH4 (ammonium) [mg/l]	V	V	V
PO4 (fosfaat) [mg/l]		V	V
pH [eenheidsloos]		V	V
Geleidbaarheid			V
NO3 (nitraat)	V		V
O2 (zuurstof)	V		
Temperatuur	V		
Niveau	V	V	V

Tabel 2: Inventarisatie RWZI parameters

Voor waterkwaliteit is NH4 de ideale parameter omdat deze op alle drie de locaties aanwezig is. Echter uit onderzoek naar de sensoren is gebleken dat NH4 sensoren iedere twee weken opnieuw gekalibreerd moeten worden hetgeen niet wenselijk is voor dit project.

De volgende sensoren zijn geselecteerd.

WS	Locatie	Soort	Parameter	Sensortype
WSHA	Scheve Klap	Waterkwantiteit	Waterpeil	Niveausensor Klay HydroCer-Kabel(10m)-VM- 6mWK
		Waterkwaliteit	Temperatuur	Temperatuursensor Klay TT-Kabel(10)-3-draads
WSBD	Chaam	Waterkwantiteit	Waterpeil	Niveausensor Klay HydroCer-Kabel(10m)-VM- 6mWK
		Waterkwaliteit	pH	Eijkelkamp AP-2000-D
WSAM	Dinther	Waterkwantiteit	Waterpeil	Niveausensor Klay HydroCer-Kabel(10m)-VM- 6mWK
		Waterkwaliteit	pH	Eijkelkamp AP-2000-D

Tabel 3: Selectie sensoren

Ook de pH sensoren zullen met enige regelmaat opnieuw gekalibreerd moeten worden. Dit is echter op een veel lager interval dan de NH4 sensoren waardoor deze wel geschikt zouden moeten zijn voor dit project.

3.4 Locatie RWZI Chaam

In overleg met de beheerder van waterschap Brabantse Delta zijn beide kasten aan het hekwerk bij de influentkelder gemonteerd. De niveausensor is door de ring onderin de put gehangen en de hoogte is bepaald door de sensor te laten zakken tot de bodem en daarna iets terug omhoog te halen. Daarna is de kabel gemonteerd in de klemhaak welke met een tie-wrap aan de ophanghaak is bevestigd.

Figuur 14: Voorzijde, achterzijde en binnenkant

De pH-sensor is met tie-wraps aan de bestaande pH-sensor van het waterschap gemonteerd en de kabel is met tie-wraps aan de buis van deze pH-sensor bevestigd.

Figuur 15: Bevestiging sensoren

Van beide kasten is, na montage van kast en sensor, de stroom gemeten. Beide gaven een betrouwbare waarde af. Ook is in eerste instantie de test-LoRa node

aangesloten om snel een meting te krijgen voor weergave op de website. Daarna zijn de definitieve LoRa nodes aangesloten. De registraties komen binnen op het Web-portal.

3.5 Locatie RWZI Heeswijk Dinther

3.5.1 Influentkelder

In overleg met de beheerder van waterschap Aa en Maas hebben we de niveausensor in een bestaande meetbuis geplaatst en door middel van de klemhaak bevestigd. De niveausensor hangt net boven de bodem van de put. Daarna is gecontroleerd of sensor correct functioneert. De gemeten stroomwaarde bedraagt in actieve periode 4 mA. De registraties komen ook binnen op het Web-Portal. Het lijkt erop dat er wat verzanding is in de hoek waar de sensor hangt.

Figuur 16: Voorzijde, achterzijde en binnenkant

De kast is met beugels bevestigd op de bij de put aanwezige paal waar ook een besturingskast op is gemonteerd.

3.5.2 Zandvanger

In overleg met de beheerder van waterschap Aa en Maas hebben we de pH-sensor met behulp van tie-wraps bevestigd aan de bestaande pH-sensor, tevens zijn de kabels aan elkaar vastgemaakt met tie-wraps. Daarna is gecontroleerd of sensor correct functioneert, dit was het geval. De gemeten stroomwaarde bedraagt in actieve periode ongeveer 15 mA. De registraties komen ook binnen op het Web-Portal.

Figuur 17: Bevestiging en locatie pH-sensor

De kast is met beugels bevestigd op het hekwerk naast de besturingskast.

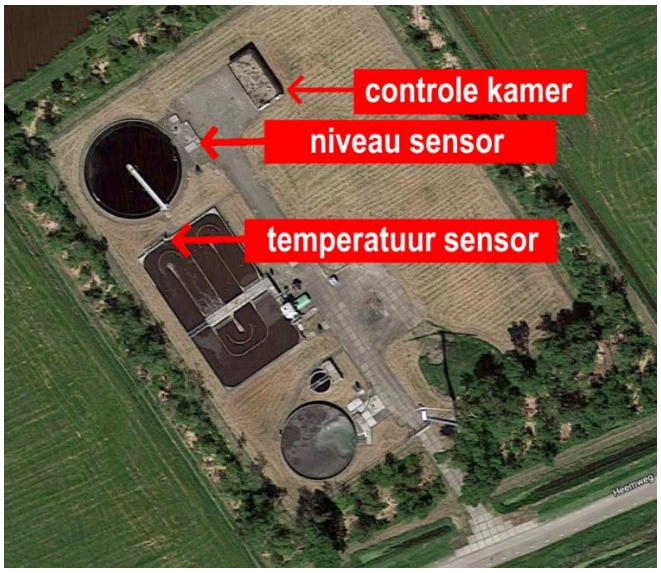
Figuur 18: Voorzijde Connection Box

Figuur 19: Achterzijde en binnenkant Connection Box

3.6 Locatie RWZI Scheve Klap

De opstelling op RWZI Scheve Klap wordt op basis van private LoRa uitgelezen. RWZI Scheve Klap heeft een gebouwtje waar de procesautomatisering (SCADA-systeem) staat opgesteld. Er is besloten om de LoRa Gateway en de andere apparatuur hier neer te zetten dichtbij de sensoren om de opstelling simpel te houden. We doen immers geen onderzoek naar hoe je zo goed mogelijk een privaat sensornetwerk kunt opbouwen. Dat valt buiten scope van dit project en bovendien zijn daar al andere partijen mee bezig[15].

[15] Zie http://www.lora-drenthe.nl



Figuur 20: Opstelling sensoren op RWZI Scheve Klap (Bron: Google Maps)

Op RWZI Scheve Klap zijn twee opstellingen geplaatst: één voor temperatuurmeting en één voor niveaumeting. De luchtfoto van Figuur 20 geeft de positie weer waar de meetopstellingen zijn geplaatst.

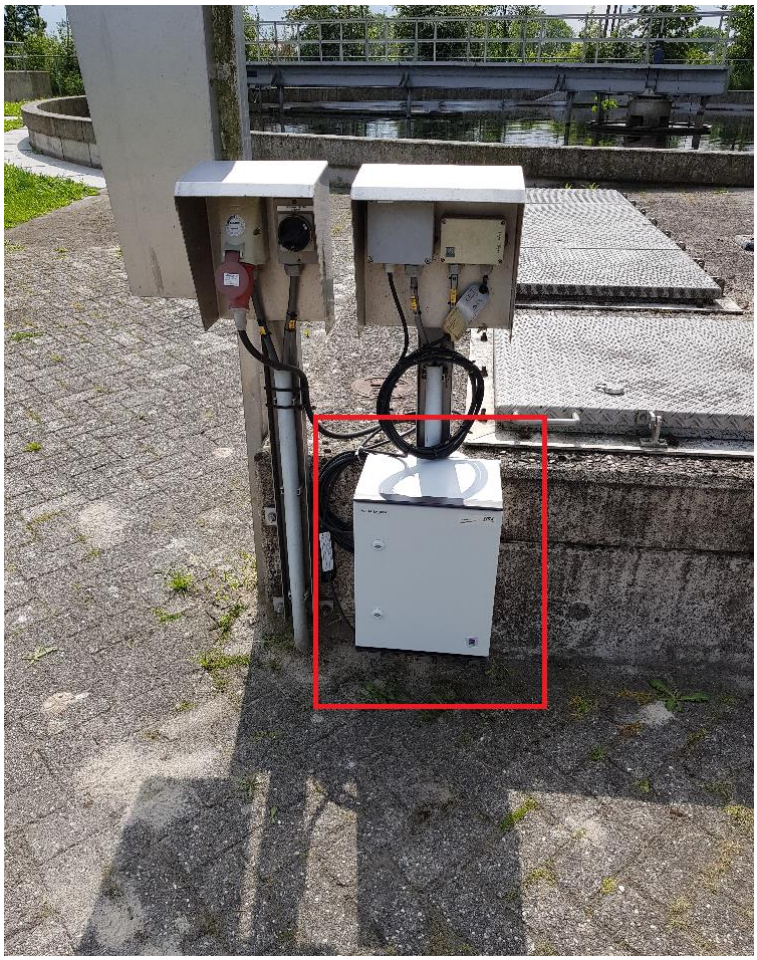
In overleg met de beheerder van waterschap Hunze en Aa's hebben we de temperatuursensor met behulp van tie-wraps bevestigd aan de bestaande temperatuursensor, tevens zijn de kabels aan elkaar vastgemaakt met tie-wraps. De kast is aan het nabij gelegen hekwerk gemonteerd met behulp van de ophangbeugels. Daarna is gecontroleerd of de sensor correct functioneert, dit was het geval. De gemeten stroomwaarde bedraagt in actieve periode ongeveer 14,26 mA. De registraties komen ook binnen op de Web-Portal van de Private LoRa omgeving.

Figuur 21: Bevestiging temperatuursensor en locatie Connection Box

Daarna is de kast voor de niveaumeting geplaatst bij de desbetreffende put en ook hier is de sensor op de bestaande sensor vastgemaakt met behulp van tie-wraps. Daarna is gecontroleerd of sensor correct functioneert, dit was het geval. De gemeten stroomwaarde bedraagt in actieve periode ongeveer 6,45 mA. De registraties komen ook binnen op het Web-Portal van de Private LoRa omgeving.

Figuur 22: Bevestiging en binnenkant Connection Box

Figuur 23: De geplaatste Connection Box bij de beluchtingsbak



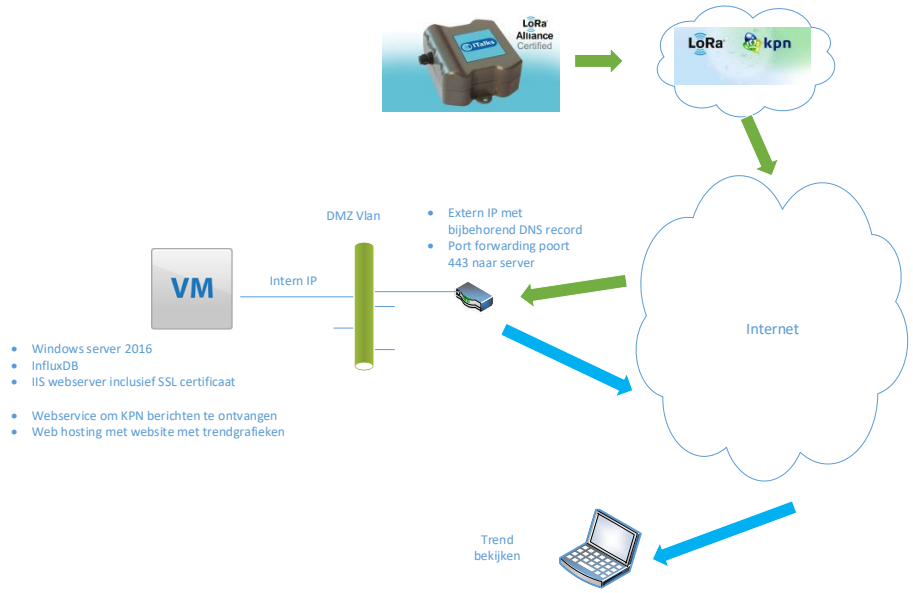
Figuur 24: De geplaatste Connection Box bij de influentput

4 Gebruikte sensornetwerken

4.1 Publiek sensornetwerk

Met publiek sensornetwerk wordt in de context van dit project bedoeld dat het LoRa radioverkeer door een commerciële netwerkbeheerder (‘managed network’) wordt opgevangen en wordt doorgestuurd naar de LoRa applicatieserver van de klant. In dit project wordt daarvoor het LoRa netwerk van KPN gebruikt. Dit houdt in dat een gebruiker een abonnement bij KPN moet afsluiten en een account krijgt om bij KPN sensor nodes en applicaties te kunnen beheren zodat het netwerk van KPN weet welk verkeer waarheen gestuurd moet worden.

De LoRa nodes in de Connection Box zijn aangemeld op het KPN LoRaWAN platform. Bij Croonwolterendros in Eindhoven is een applicatie aan het internet gekoppeld waar de sensorberichten naartoe worden verstuurd.



Figuur 25: Publiek sensornetwerk

Als het LoRa radiobericht door drie of meer antennemasten wordt ontvangen, stuurt KPN ook de locatiegegevens mee. Dit hebben we ook verwerkt in de applicatie.

4.1.1 Benodigdheden

De volgende zaken zijn ingericht:

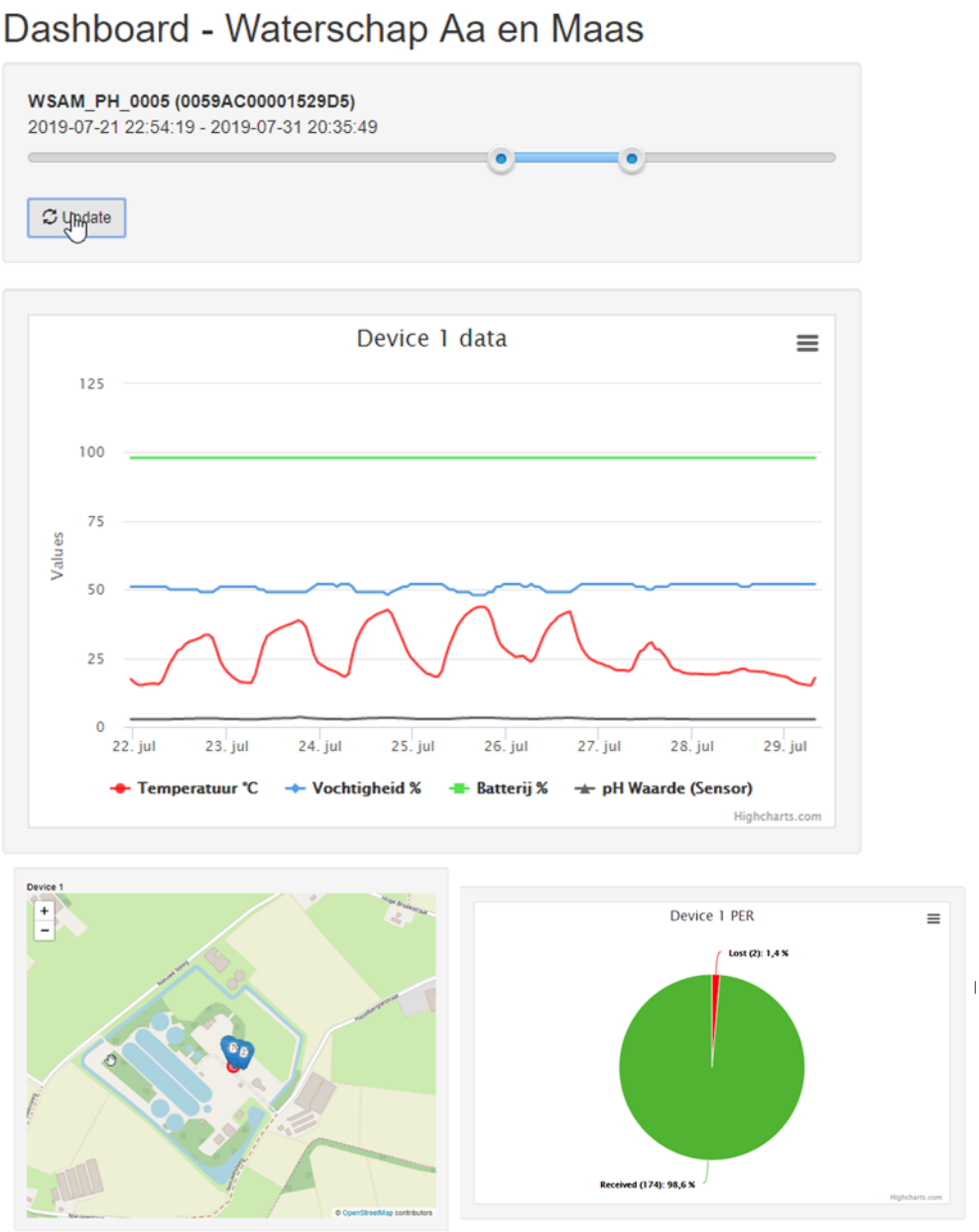
- Nodes geconfigureerd
- Nodes aangemeld bij het KPN LoRaWAN platform
- Domeinnaam aangevraagd (tkilora.nl)
- SSL certificaat aangevraagd
- Firewall geconfigureerd
- Virtuele server met Windows Server 2016 ingericht
- Applicaties ingericht

4.1.2 Applicaties

Op de virtuele server zijn drie applicaties geïnstalleerd:

- InfluxDB om de gegevens op te slaan
- Webservice om de LoRaWAN berichten van KPN te ontvangen
- Website met trend objecten om de meetwaarden uit influxDB te visualiseren.

Beide applicaties zijn gemaakt met Microsoft technologie en maken gebruik van een ‘trend-object’ bibliotheek.



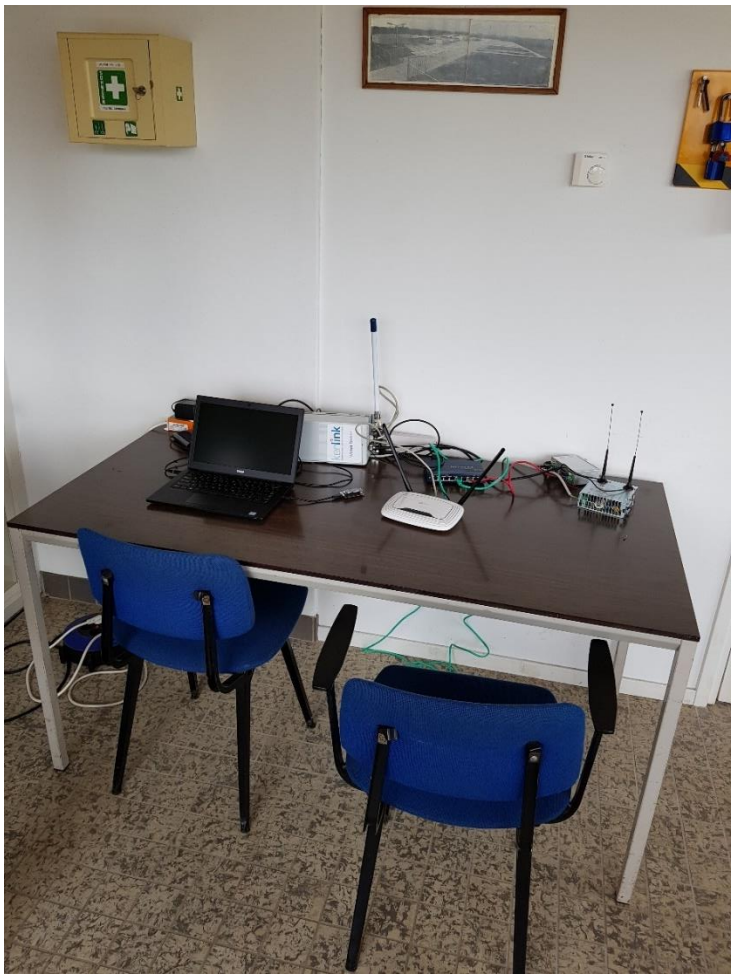
Figuur 26: Screenshots van de webapplicatie

Aan de bovenkant (zie Figuur 26) van de User Interface kan met een slider het datumbereik worden geselecteerd zodat de meetwaardes voor een periode kunnen worden getoond. Linksonder worden de locatiegegevens getoond en rechtsonder

een PIE chart met de hoeveelheid ontvangen berichten ten opzichte van het aantal te verwachten berichten.

4.2 Privaat sensornetwerk

Een typische LoRaWAN sensorketen bestaat uit een LoRa node, een LoRa gateway, een netwerkserver, een applicatieserver en de applicatie van de eindgebruiker. Voor het private sensornetwerk is gekozen om de gehele opstelling op locatie te plaatsen. Hiervoor is een klein testnetwerk ingericht (zie Figuur 27) dat bestaat uit een laptop om de netwerk- en applicatie server te draaien, een WiFi router om de laptop en gateway te verbinden en een industriële gateway met SIM kaart om de sensor data te ontsluiten naar TNO en voor remote toegang om deze opstelling op afstand te kunnen beheren.



Figuur 27: Privaat sensornetwerk

4.2.1 Nodes

De node is de Connection Box voorzien van sensoren zoals die beschreven zijn in hoofdstuk 3. De hardware en software aan de sensor kant is gelijk aan die van de publieke opstelling, echter zijn ze voorzien van een specifieke *ApplicationKey*.

4.2.2 LoRa Gateway

Op locatie is een enkele Kerlink Wirnet Station[16] geplaatst. Deze gateway draait een linux operating systeem en is voorzien van een *packet forwarder* van Semtech die geconfigureerd is om via UDP de ontvangen LoRa pakketten te versturen naar de netwerkserver. Een netwerkkabel voorziet de gateway van stroom en een directe verbinding met de router.

4.2.3 Server architectuur

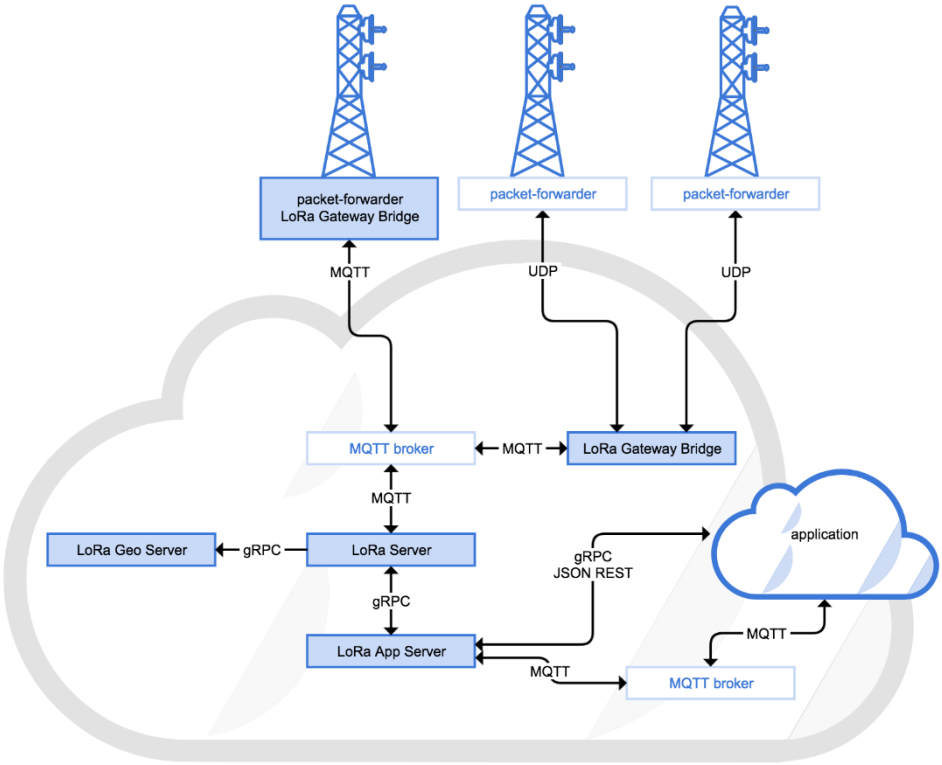
Voor het server gedeelte van de opstelling is er voor gekozen om de software opstelling van *LoraServer*[17] te gebruiken. Meerdere oplossingen zijn onderzocht, waaronder ook de software van The Things Netwerk[18], maar ten tijde van de bouw van het netwerk bood LoraServer een complete open-source oplossing van de belangrijkste bouwblokken. Daarnaast was een belangrijk pluspunt de uitgebreide documentatie en de management web interface waardoor we een eigen sensornetwerk konden samenstellen.

De illustratie uit de documentatie van LoraServer (zie Figuur 28) geeft een goed overzicht van de gebruikte onderdelen. De LoraServer maakt voor veel van haar communicatie gebruik van MQTT[19], een protocol dat binnen IoT oplossingen veel gebruikt wordt voor het uitwisselen van berichten. Omdat in deze opstelling de packet forwarder geconfigureerd is om de LoRa berichten over UDP te versturen, is er een extra *LoRa Gateway Bridge* voor het omzetten van deze berichten naar het MQTT protocol. Een van de voordelen van deze tussenstap is dat de LoRa server nu alleen een beveiligde verbinding met de MQTT broker hoeft te onderhouden.

Een andere mogelijkheid was geweest om een eigen packet forwarder op de gateway te gebruiken en deze direct via MQTT met de broker te laten

[16] https://www.kerlink.com/product/wirnet-station/
[17] https://www.loraserver.io
[18] https://www.thethingsnetwork.org/
[19] https://en.wikipedia.org/wiki/MQTT

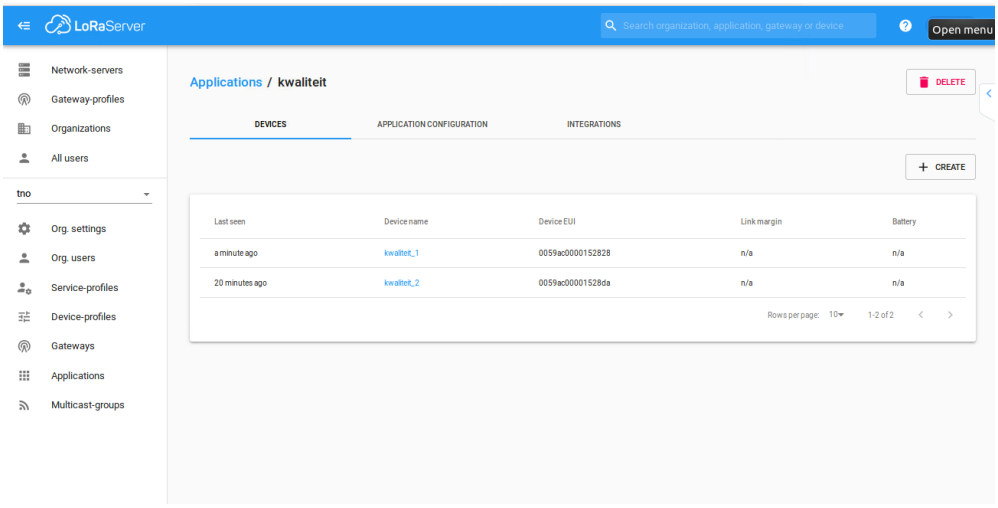
communiceren. Hiervoor is niet gekozen om zo dicht mogelijk te blijven bij de oplossing zoals die geleverd wordt door de leverancier van de gateway.



Figuur 28 LoraServer architectuur

De LoRa server is verantwoordelijk voor het beheer van het LoRaWAN netwerk en heeft daarmee kennis van de gateways en nodes die mogen verbinden, handelt de aanvragen af van nodes die willen verbinden met het netwerk en zet eventuele berichten door die naar de nodes verzonden moeten worden. Mochten er meerdere gateways aangesloten zijn die allemaal hetzelfde bericht van een LoRa node ontvangen, dan worden deze door de LoRa server ‘ontdubbeld’.

Het beheer van de gateways en nodes gebeurt in de *LoRa App Server*. Via een web interface kan de gebruiker inloggen, organisaties aanmaken, gateways en applicaties registreren om uiteindelijk nodes te configureren.



Figuur 29 Device beheer in applicatie server

De volledige server opstelling op locatie draait op een laptop die is voorzien van Ubuntu Linux. Alle gebruikte LoraServer componenten draaien als Docker containers en zijn in een docker-compose[20] geconfigureerd om eenvoudig en consistent te kunnen starten.

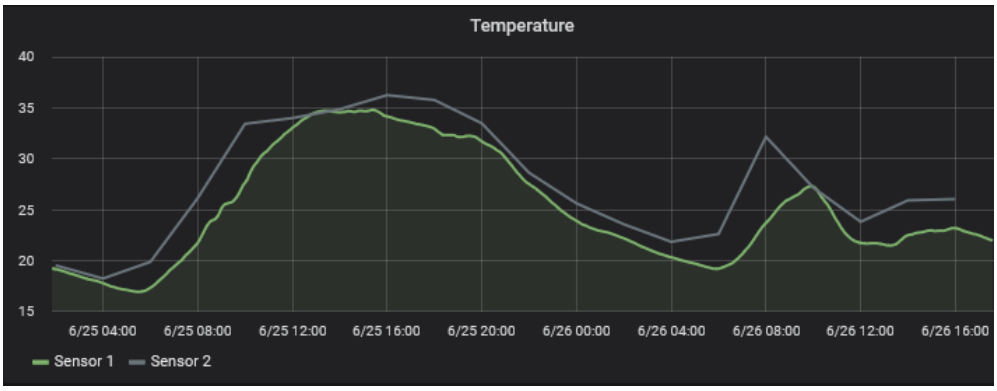
4.2.4 Applicatie

De application server biedt ook enkele integratie mogelijkheden aan om de data van de nodes direct door te zetten naar een applicatie van de eindgebruiker. Hiervoor moet de server dan wel worden voorzien van source code om de sensor data te parsen en om te zetten naar leesbare sensordata. In het geval van de sensoren in de Connection Box ziet de javascript code er als volgt uit.

```
function Decode(fPort, bytes) {
  return {
    bytes: String(bytes),
    temperature:((bytes[1] * 256) + bytes[2])/100,
    humidity:bytes[3],
    battery:bytes[4],
    val:((bytes[5]*256) + bytes[6])/1000
  };
}
```

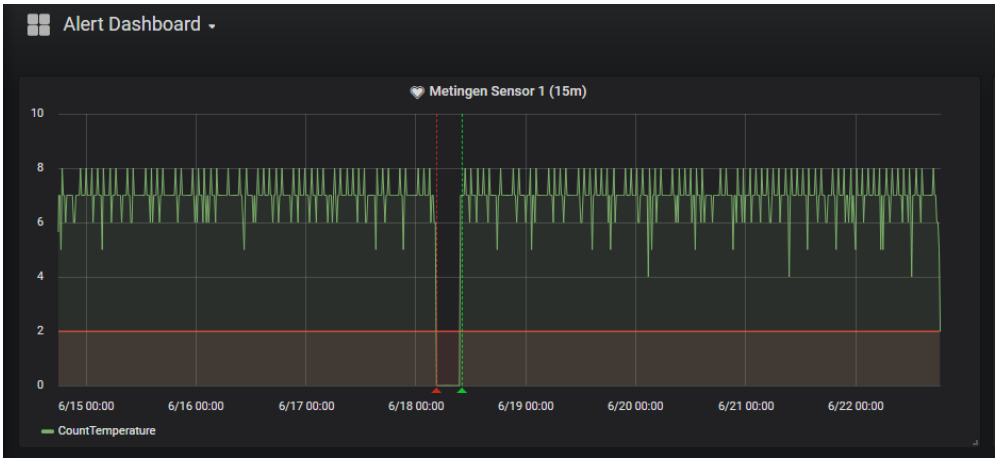
Voor het opslaan en visualiseren van de data is er een server bij TNO ingericht met een database (InfluxDB) die direct gekoppeld kan worden met de applicatie server. Bovenop deze database is met software van Grafana een dashboard gemaakt om de sensor data te visualiseren (zie Figuur 30).

[20] https://www.loraserver.io/guides/docker-compose/



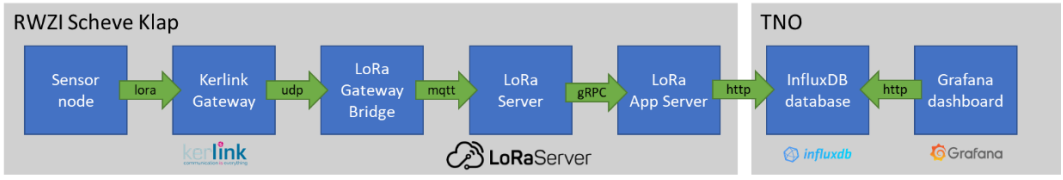
Figuur 30 Sensor dashboard (ITALKS MCS 1608 temperatuur sensor)

In Grafana is ook een Alert Dashboard ontwikkeld voor het monitoren van de frequentie waarmee de metingen binnen komen. Zodra de frequentie onder een ingesteld minimum komt, wordt er via Slack een notificatie verstuurd.



Figuur 31 Monitor dashboard met alert functie

De volledige sensorketen zoals hierboven beschreven, ziet er als volgt uit:



Figuur 32 Overzicht complete keten van sensor tot dashboard

5 Onderzoeksresultaten

Er zijn in totaal zes veldopstellingen geplaatst bij drie verschillende waterschappen. Per locatie zijn twee opstellingen neergezet:

- Eén opstelling voor het meten van het waterniveau (waterkwantiteit).
- Eén opstelling voor het meten van een fysische parameter (waterkwaliteit).

WS	Locatie	Soort	Parameter	LoRa netwerk
WSHA	Scheve Klap	Waterkwantiteit	Waterpeil	Privaat LoRaWAN
		Waterkwaliteit	Temperatuur	Privaat LoRaWAN
WSBD	Chaam	Waterkwantiteit	Waterpeil	KPN LoRaWAN
		Waterkwaliteit	pH	KPN LoRaWAN
WSAM	Dinther	Waterkwantiteit	Waterpeil	KPN LoRaWAN
		Waterkwaliteit	pH	KPN LoRaWAN

Tabel 4: Locatie Chaam en Dinther gebruiken KPN LoRaWAN

De twee locaties Chaam en Dinther maken gebruiken van het KPN LoRaWAN netwerk voor het versturen van sensordata en de locatie Scheve Klap maakt gebruik van een privaat LoRaWAN netwerk (zie Tabel 4).

De functionele test-scenario's zijn uitgevoerd op al deze sensornetwerken in het veld, dus zowel de publieke als de private variant. De security test-scenario's zijn alleen uitgevoerd op de private variant in het lab. Deze private variant voor in het lab is volledig los gehouden van de veldopstellingen en is in de lab-omgeving van Applied Risk geplaatst.

5.1 Analyse publiek sensornetwerk (KPN)

5.1.1 Betrouwbaarheid

Over de maand juni 2019 is een datareeks van de WSBD en een datareeks van de WSAM opstelling bekeken. De klantserver heeft er in deze periode twee dagen uitgelegen, tussen 12 juni 16.00u en 14 juni 16.00u. Als we dit interval buiten beschouwing laten[21], kan worden berekend hoeveel metingen er zijn ontvangen en hoeveel er ontbreken. De verzend-frequentie van de LoRa-loggers die geïnstalleerd zijn bij de RWZI's is ingesteld op één meting per uur.

Bij de WSAM opstelling ontbreken 25 metingen en bij de WSBD opstelling ontbreken er 7. Uitgaande van een meetperiode van 28 dagen * 24 metingen = 672 dan is bij WSBD 665 / 672 * 100% = 98,9 % aangekomen en bij WSAM is 647 / 672 * 100% = 96,2% aangekomen. Er is geen verband gevonden tussen de verschillende opstellingen voor de ontbrekende metingen.

[21] Een storing in de klantserver kan LoRa niet worden aangerekend.

DateTime	Temperatuur	Vochtigheid	Batteri	Waterniveau in milimeters (Sens	mist
2019-06-08 09:25:50	12.5	44,00	99,00	50830078125,00	vorige meting mist
2019-06-17 13:56:00	25.44	46,00	99,00	521484375,00	vorige meting mist
2019-06-18 12:00:01	25.01	47,00	99,00	662109375,00	vorige meting mist
2019-06-19 06:02:29	16.43	48,00	99,00	59765625,00	vorige meting mist
2019-06-24 22:21:08	27.49	50,00	99,00	64306640625,00	vorige meting mist
2019-06-25 21:24:17	30.15	50,00	99,00	6884765625,00	vorige meting mist
2019-06-30 21:40:44	23.62	52,00	99,00	60498046875,00	vorige meting mist

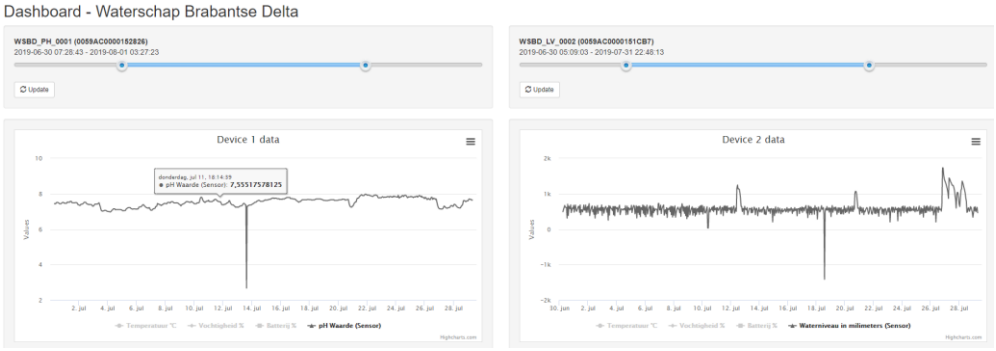
Figuur 33: WSBD missende metingen

DateTime	Temperatuur	Vochtigheid	Batteri	pH Waarde (Sens	mist
2019-06-02 03:29:57	14.93	42,00	99,00	48203125,00	vorige meting mist
2019-06-02 17:32:49	34.32	41,00	99,00	557763671875,00	vorige meting mist
2019-06-03 04:34:20	16.71	43,00	99,00	46533203125,00	vorige meting mist
2019-06-04 00:37:04	14.85	43,00	99,00	4626953125,00	vorige meting mist
2019-06-05 12:41:59	19.7	42,00	99,00	45654296875,00	vorige meting mist
2019-06-07 13:48:41	25.44	42,00	99,00	473681640625,00	vorige meting mist
2019-06-07 18:49:34	18.6	43,00	99,00	4322265625,00	vorige meting mist
2019-06-10 06:57:38	13.27	44,00	99,00	408349609375,00	vorige meting mist
2019-06-10 16:59:00	26.19	43,00	99,00	469287109375,00	vorige meting mist
2019-06-11 13:01:44	23.31	44,00	99,00	429736328125,00	vorige meting mist
2019-06-20 12:32:07	21.24	46,00	99,00	36689453125,00	vorige meting mist
2019-06-20 19:33:09	22.85	47,00	99,00	375830078125,00	vorige meting mist
2019-06-21 04:34:19	11.21	47,00	99,00	3490234375,00	vorige meting mist
2019-06-21 23:37:11	13.66	48,00	99,00	36044921875,00	vorige meting mist
2019-06-22 01:37:08	11.28	48,00	99,00	3501953125,00	vorige meting mist
2019-06-23 04:40:53	13.62	48,00	99,00	325732421875,00	vorige meting mist
2019-06-23 10:41:44	29.85	46,00	99,00	347998046875,00	vorige meting mist
2019-06-25 23:50:00	25.39	48,00	99,00	388720703125,00	vorige meting mist
2019-06-27 09:54:38	21.53	48,00	98,00	3583984375,00	vorige meting mist
2019-06-27 12:55:08	25.89	48,00	98,00	370556640625,00	vorige meting mist
2019-06-28 05:57:22	10.13	49,00	98,00	34052734375,00	vorige meting mist
2019-06-29 02:00:06	14.93	49,00	98,00	352099609375,00	vorige meting mist
2019-06-30 02:03:23	19.8	50,00	98,00	36748046875,00	vorige meting mist
2019-06-30 09:04:24	28.22	48,00	98,00	37099609375,00	vorige meting mist
2019-06-30 18:05:56	30.43	48,00	98,00	381103515625,00	vorige meting mist

Figuur 34: WSAM missende metingen

5.1.2 Screenshot maand juli

Na de voor dit project afgesproken meetperiode van juni 2019 hebben de opstellingen tijdens de verwerking van de resultaten en het opstellen van de documentatie nog gedraaid in de maand juli 2019 (zie Figuur 35).



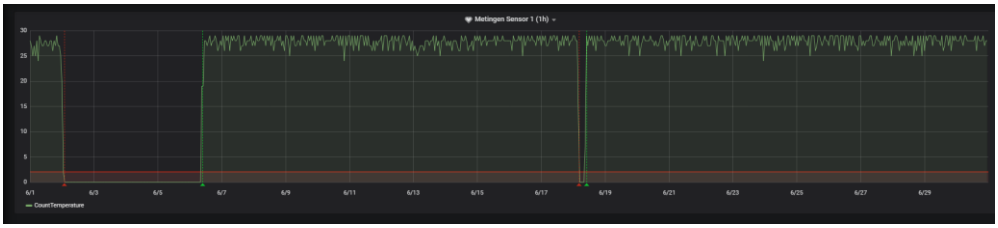
Figuur 35 : WSBD links PH en rechts Niveau

Er is mooi te zien dat het flink heeft geregend eind juli 2019[22] op de betreffende locatie. Daarnaast valt op dat in beide grafieken lange uitschieters naar beneden zitten. Dit zijn incorrecte metingen waarvan de oorzaak nog niet is achterhaald.

5.2 Analyse privaat sensornetwerk

5.2.1 Betrouwbaarheid

In de meetperiode in de maand juni 2019 is er tweemaal een storing opgetreden, zoals ook te zien is in het monitor dashboard (Figuur 36). De eerste keer betrof het een netwerkconfiguratie fout in onze proefopstelling op locatie bij de RWZI Scheve Klap. De router had de verbinding met de LoRa gateway verbroken en niet hersteld na een DHCP conflict. Dit probleem is opgelost door de Kerlink gateway een vast IP adres te geven. Na deze aanpassing heeft de LoRa opstelling de rest van de meetperiode zonder problemen gefunctioneerd. De tweede storing was te wijten aan een stroomstoring in een switch in de labomgeving van TNO. Hierdoor was de database gedurende vijf uur niet bereikbaar.



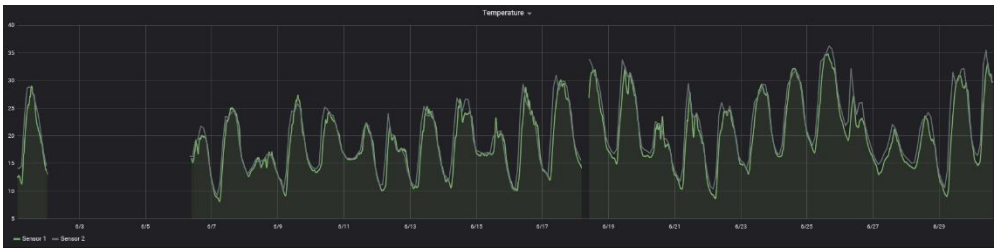
Figuur 36 Alert dashboard

Door deze storingen is het totaal aantal ontvangen metingen lager dan verwacht zou mogen worden. Voor de meting van het waterniveau[23] hebben we 599 metingen ontvangen ten opzichte van 720 te verwachten metingen op basis van 30 dagen x 24 uur x 1 meting per uur. Dat komt overeen met 83%. Voor een week zonder storingen ligt dit percentage op 97%. Voor de meting van de watertemperatuur[24] hebben we 17004 metingen ontvangen ten opzichte van 21600 te verwachten metingen op basis van 30 dagen x 24 uur x 30 metingen per uur. Dat komt overeen met 78%. Voor een week zonder storingen ligt dit percentage op 93%.

[22] Zie https://www.knmi.nl/nederland-nu/klimatologie/geografische-overzichten/archief/maand/rd
[23] Sensor stuurt metingen eens per uur (lage frequentie)
[24] Sensor stuurt metingen om de 2 minuten (hoge frequentie)

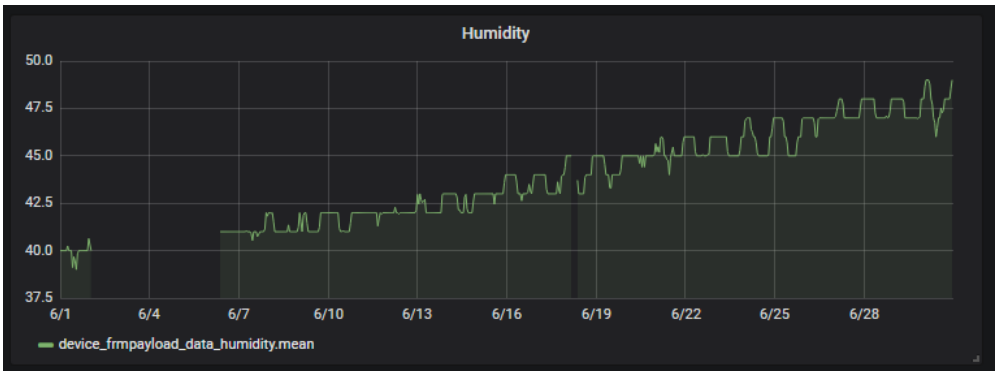
5.2.2 Resultaten sensoren

De volgende grafieken tonen enkele resultaten zoals die verzameld zijn over meetperiode waarbij sommige meetreeksen in Grafana gecombineerd zijn.



Figuur 37 Temperatuur van de twee LoRa nodes

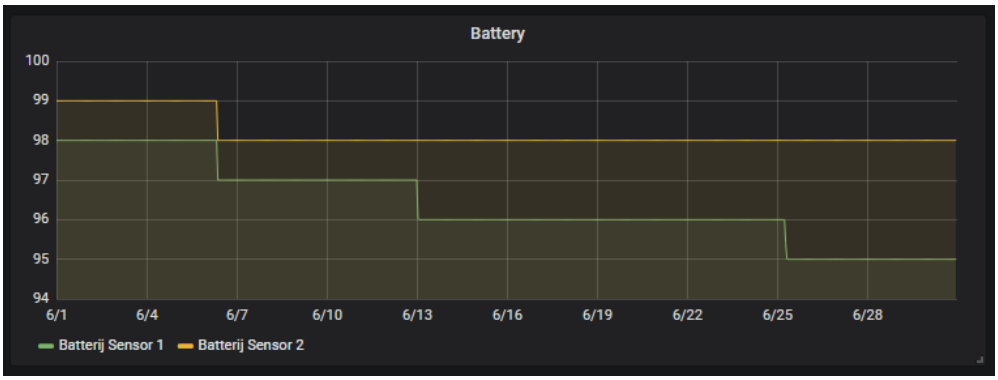
In bovenstaande gecombineerde grafiek (zie Figuur 37) wordt de temperatuur weergegeven over de hele maand juni 2019 op RWZI Scheve Klap zoals gemeten met de interne temperatuursensor van de ITALKS MCS 1608 LoRa node. Dit is de temperatuur ín de afgesloten Connection Box 1 en 2, dus niet van de beluchtingsbak of de influentput.



Figuur 38 Vochtigheid sensor 1, gehele meetperiode

Opvallend bij de metingen met betrekking tot vochtigheid, ook gemeten met een interne sensor in de ITALKS MCS 1608, is dat deze gedurende de gehele meetperiode is gestegen. Volgens het KNMI was de maand juni 2019 “extreem warm, nat en zeer zonnig”[25]. Condensvorming in de Connection Box is een mogelijke verklaring voor deze grafiek.

[25] Zie https://www.knmi.nl/nederland-nu/klimatologie/maand-en-seizoensoverzichten/2019/juni



Figuur 39 Batterijstatus beide sensoren, gehele meetperiode

De batterijstatus van beide LoRa nodes (dit betreft de interne batterij van de ITALKS MCS 1608) laat mooi zien dat sensor 1 meer energie heeft verbruikt dan sensor 2. Dit is te verklaren doordat sensor 1 met een hoge frequentie rapporteert (elke 2 minuten) terwijl sensor 2 dit met een lage frequentie doet (1x per uur).

5.3 Analyse contra-metingen van de waterschappen

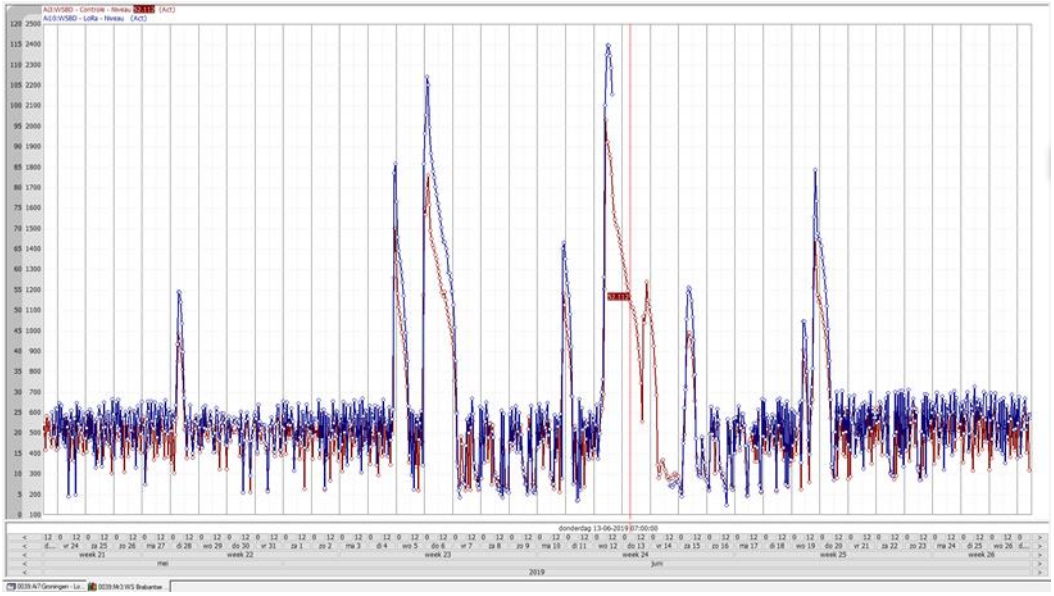
Voor de veldopstellingen worden in deze paragraaf meerdere grafieken gepresenteerd voor de verschillende gemeten watervariabelen op de drie locaties. De eerste plot is telkens een totaaloverzicht en de tweede plot is een grafiek van een week om wat te kunnen inzoomen voor wat betreft detailniveau.

De ontwikkelde industriële LoRa sensoren zijn niet gekalibreerd ten opzichte van de sensoren van de waterschappen. Ook zijn ze niet gesynchroniseerd op datum en tijd. Om de LoRa metingen toch te kunnen vergelijken met de contra-metingen van de waterschappen, zijn de grafieken over elkaar heen ‘gelegd’ met elk hun eigen y-as. Dit is om te kunnen onderzoeken of er overeenkomsten en verschillen zichtbaar zijn in de trends van de LoRa metingen en de trends van de contra-metingen.

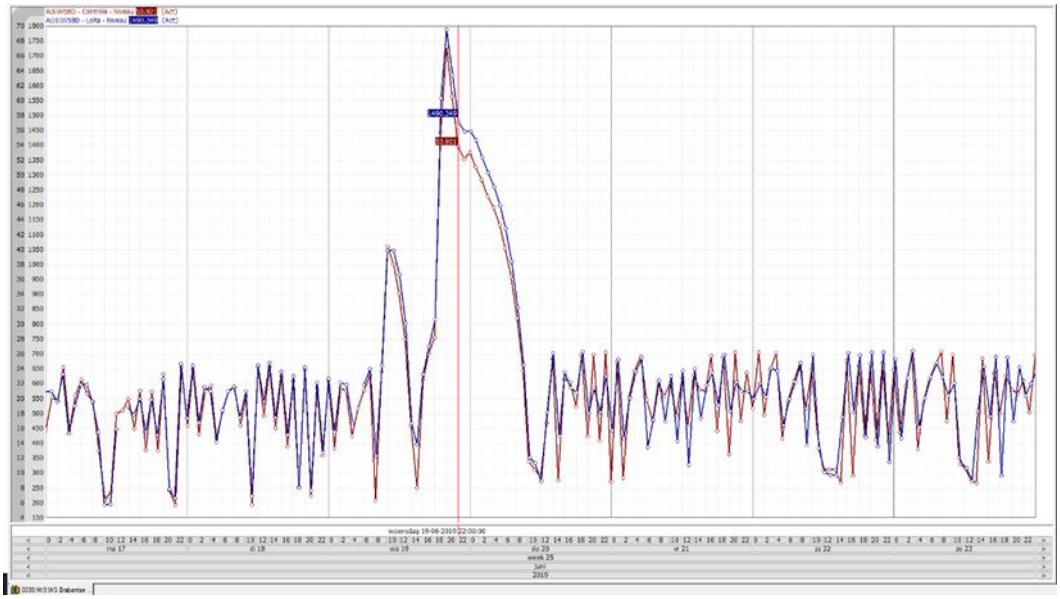
5.3.1 RWZI Chaam niveau-meting

Figuur 40 laat een overzicht zien van de data met betrekking tot de niveaumetingen in de periode van 24 mei t/m 26 juni (dus inclusief de aanloop naar de meetmaand juni 2019). De blauwe lijn geeft de gemeten waarde weer zoals gemeten met de proefopstelling met de LoRa node. De rode lijn geeft de gemeten waarden weer die ter beschikking zijn gesteld door het waterschap.

Wat opvalt in het totaaloverzicht is dat van de periode 12 t/m 14 juni de storing van de klantserver zoals aangegeven door Croonwolter&dros goed te zien is.



Figuur 40: Totaaloverzicht niveaumetingen RWZI Chaam

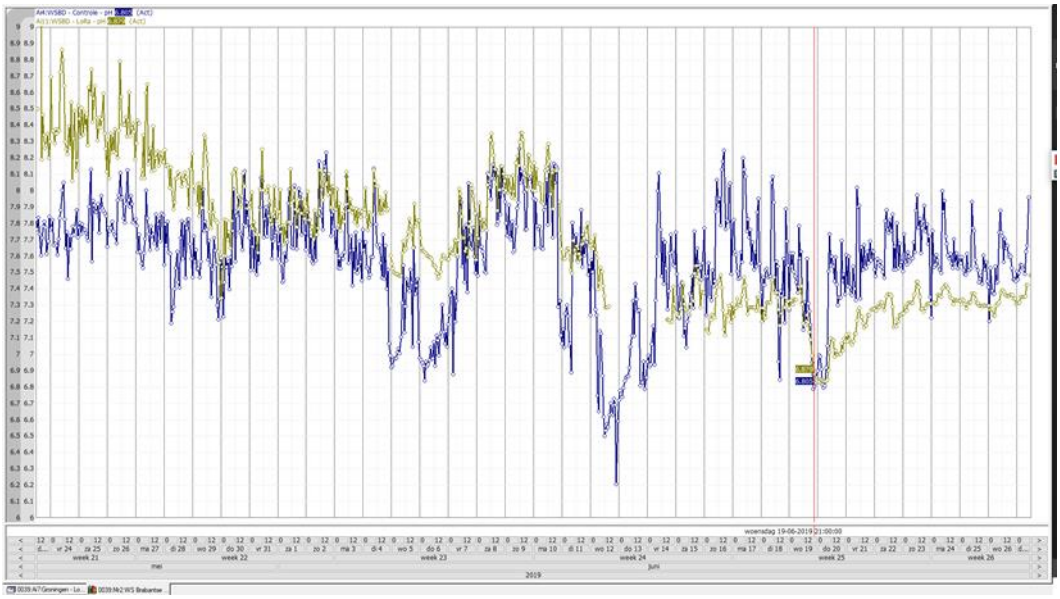


Figuur 41: Weekoverzicht niveaumetingen RWZI Chaam

Figuur 41 laat een weekoverzicht zien van de data in de periode 17 t/m 22 juni. In het weekoverzicht is goed te zien dat het trendverloop van de data in het algemeen goed te noemen is. Er zijn geen bijzondere afwijkingen. In beide plots is de trend tussen de data en de referentiemetingen duidelijk te zien.

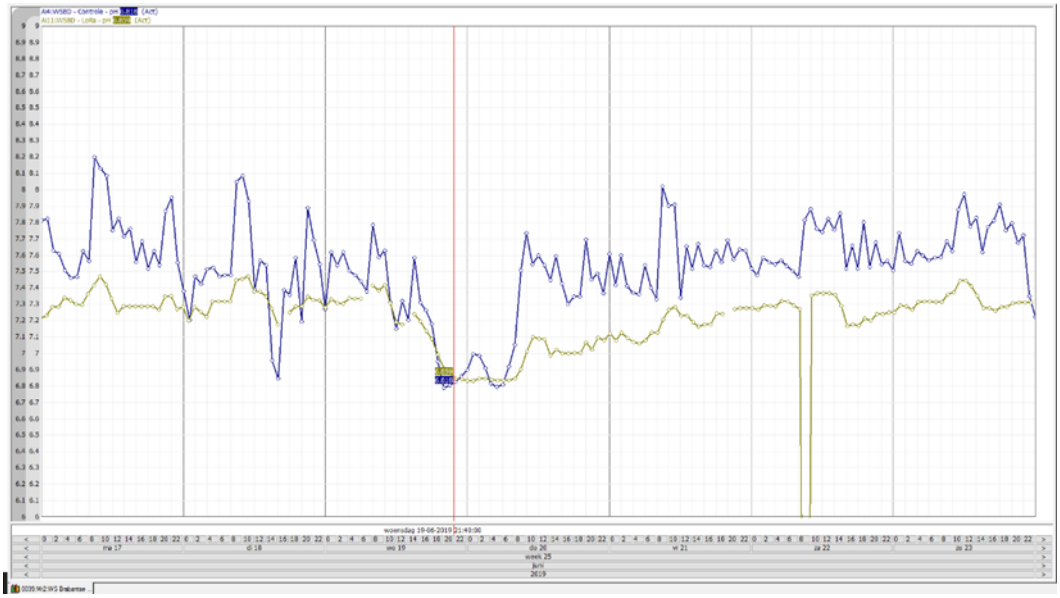
5.3.2 RWZI Chaam pH-meting

In Figuur 42 is een overzicht te zien van de data met betrekking tot de pH-metingen in de periode van 24 mei t/m 26 juni en in Figuur 43 een overzicht van de data in de periode 17 t/m 22 juni. De groene lijn geeft de gemeten waarden weer met de proefopstelling. De blauwe lijn geeft de gemeten waarden weer die ter beschikking zijn gesteld door het waterschap.



Figuur 42: Totaaloverzicht pH-waarde metingen RWZI Chaam

Wat ook hier direct opvalt in het totaaloverzicht is dat er in de periode 12 t/m 14 juni data van de LoRa node ontbreekt (groene lijn).



Figuur 43: Weekoverzicht pH-waarde metingen RWZI Chaam

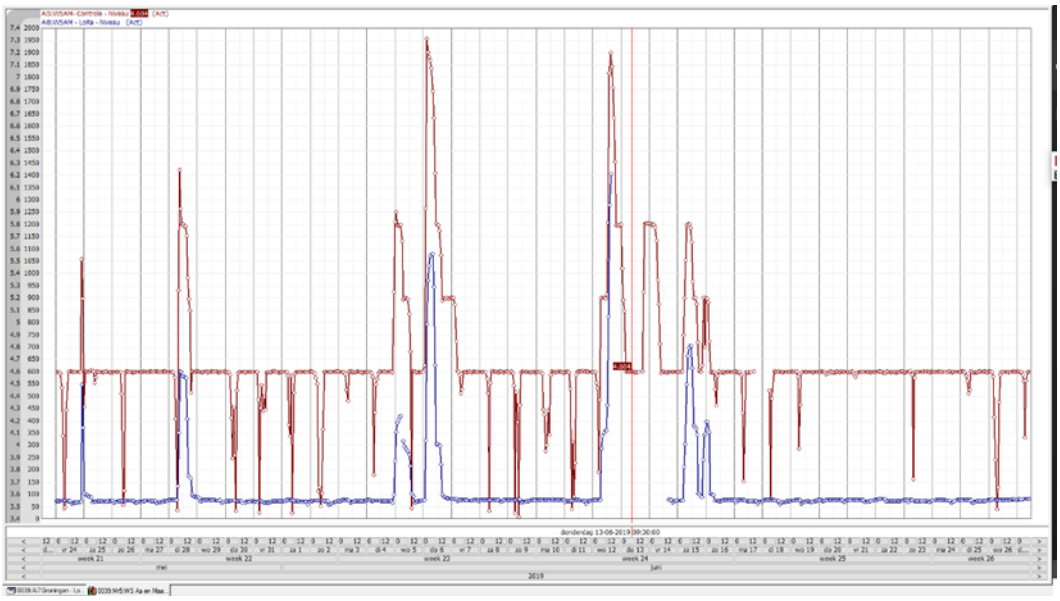
Het trendverloop van de data (zie Figuur 43) is over het algemeen goed te noemen. De trends tussen de LoRa data en de referentiemetingen zijn duidelijk te zien. De sensor van de RWZI is wel wat ‘springeriger’ dan de LoRa sensor. Op 22 juni rond 08.00 uur is één uitschieter naar beneden zichtbaar (groene lijn). De oorzaak hiervan is niet duidelijk.

5.3.3 RWZI Heeswijk Dinther niveau-meting

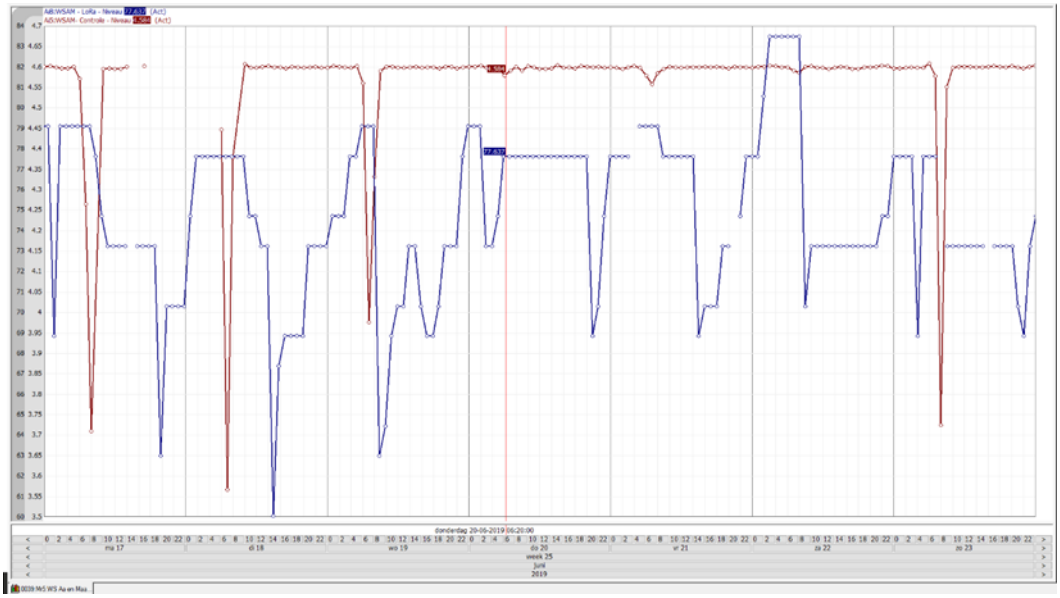
In Figuur 44 is een overzicht te zien van de data met betrekking tot de niveaumetingen in de periode van 24 mei t/m 26 juni en in Figuur 45 een overzicht van de data in de periode 17 t/m 22 juni. De blauwe lijn geeft de gemeten waarde

weer zoals gemeten met de proefopstelling met de LoRa node. De rode lijn geeft de gemeten waarden weer die ter beschikking zijn gesteld door het waterschap.

Het trendverloop van de data is in het algemeen goed te noemen met hier en daar een enkele uitschieter.



Figuur 44: Totaaloverzicht niveaumetingen RWZI Heeswijk Dinther



Figuur 45: Weekoverzicht niveaumetingen RWZI Heeswijk Dinther

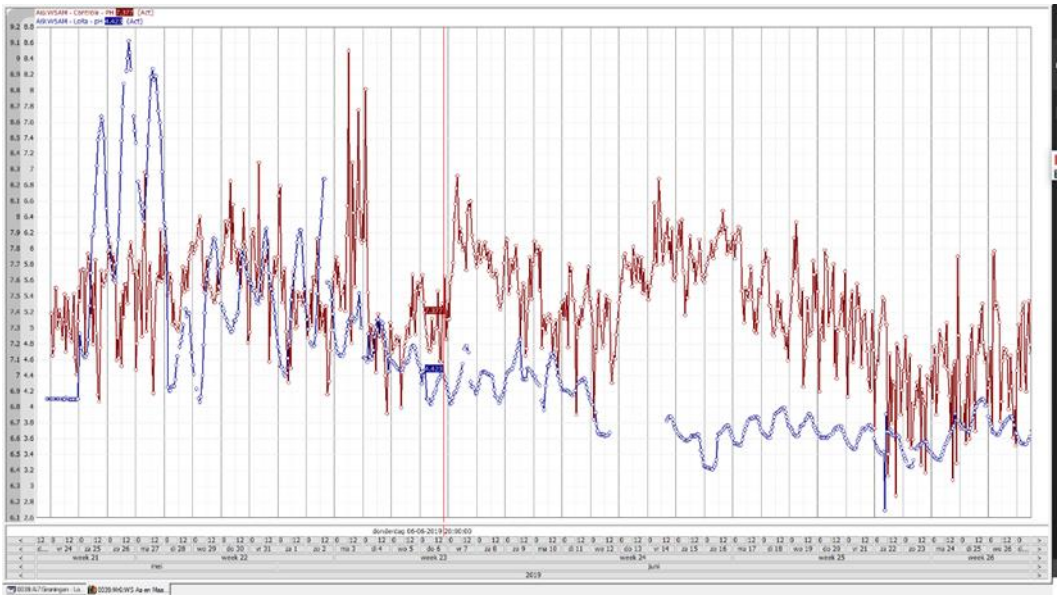
In het weekoverzicht (zie Figuur 45) is goed te zien dat er enkele metingen in de LoRa reeks ontbreken (blauwe lijn). Daarnaast ontbreekt er ook controle data in de door het waterschap toegeleverde data en wel op 17 juni (rode lijn). In de door het waterschap aangeleverde tabel wordt de datakwaliteit als zijnde “Bad” geclassificeerd. De meest waarschijnlijke oorzaak hiervan is dat er een slechte verbinding is geweest tussen het Siemens onderstation (PLC) en i-Historian

(SCADA software). In beide plotjes lijkt alleen de trend naar boven correct te zijn. Wellicht is dit te verklaren door de plaats van de sensor. Op locatie is waargenomen dat de sensor op de verzanding rust. Ook lijkt de resolutie van de A/D-converter van invloed te zijn op de grafiek want deze is nogal schokkerig.

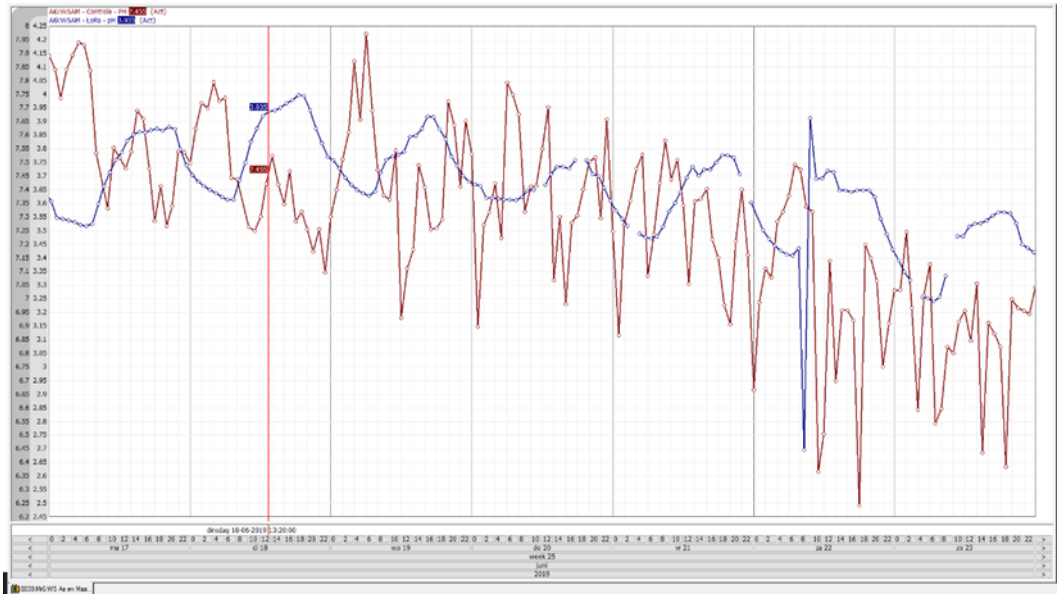
5.3.4 RWZI Heeswijk Dinther pH-meting

In Figuur 46 is een overzicht te zien van de data met betrekking tot de pH-metingen in de periode van 24 mei t/m 26 juni en in Figuur 47 een overzicht van de data in de periode 17 t/m 22 juni. De blauwe lijn geeft de gemeten waarde weer zoals gemeten met de proefopstelling met de LoRa node. De rode lijn geeft de gemeten waarden weer die ter beschikking zijn gesteld door het waterschap.

Ook in dit totaaloverzicht is dezelfde periode aan ontbrekende data te zien (blauwe lijn) zoals ook bij de proefopstellingen in RWZI Chaam. Het trendverloop van de data is in het algemeen goed te noemen met hier en daar een enkele uitschieter.



Figuur 46: Totaaloverzicht pH-metingen RWZI Heeswijk Dinther

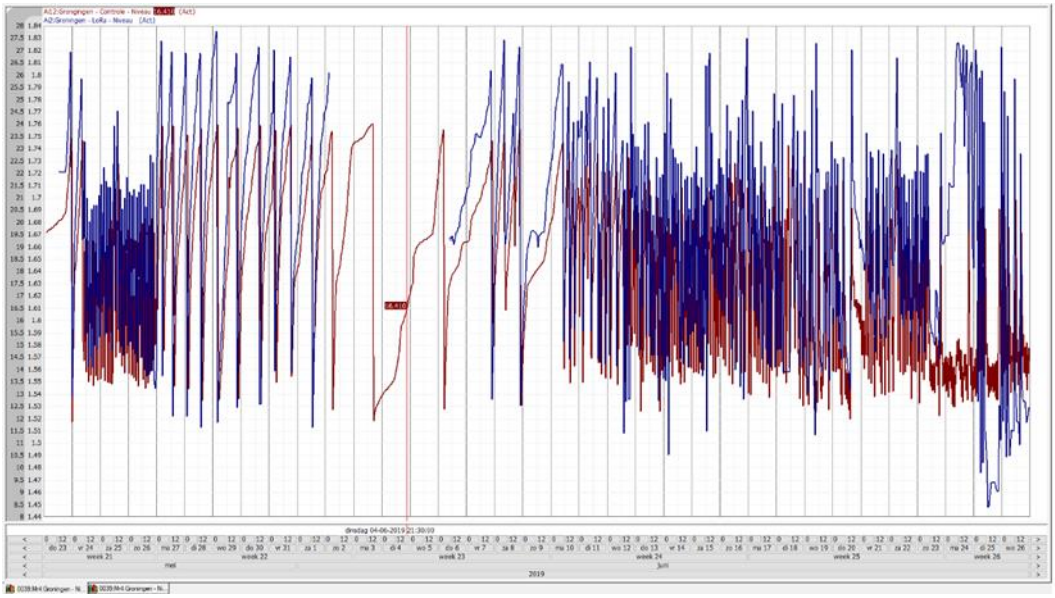


Figuur 47: Weekoverzicht pH-metingen met aangepaste schaal RWZI Heeswijk Dinther

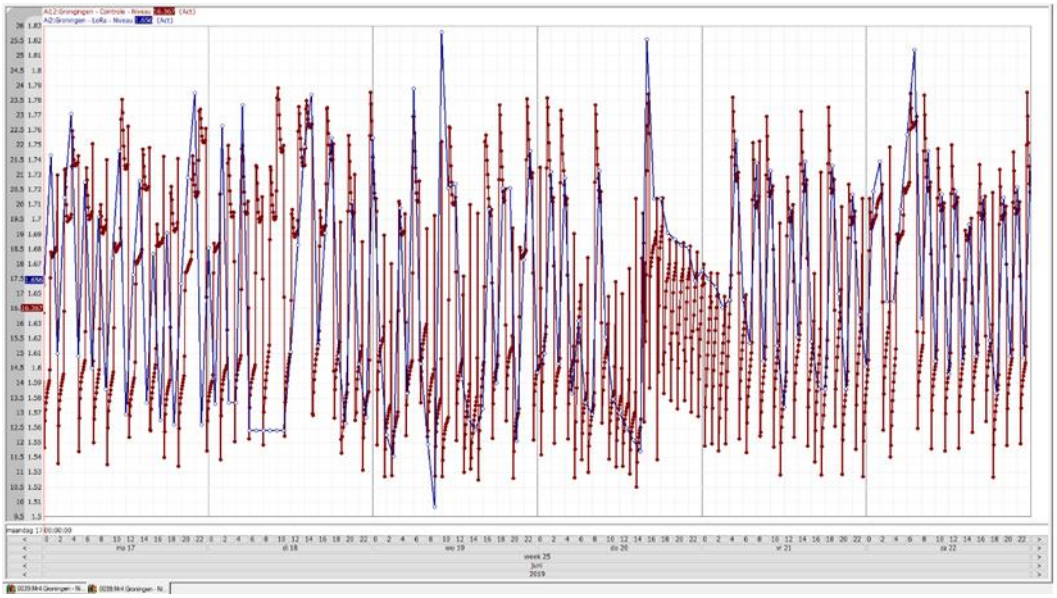
5.3.5 RWZI Scheve Klap niveau-meting

In Figuur 48 is een overzicht te zien van de data met betrekking tot de niveaumetingen in de periode van 24 mei t/m 26 juni en in Figuur 49 een overzicht van de data in de periode 17 t/m 22 juni. De blauwe lijn geeft de gemeten waarde weer zoals gemeten met de proefopstelling met de LoRa node. De rode lijn geeft de gemeten waarden weer die ter beschikking zijn gesteld door het waterschap.

Wat opvalt is dat er over een aaneengesloten periode van meerdere dagen, de periode 2 t/m 6 juni, data van de LoRa node ontbreekt zoals aangegeven door TNO (blauwe lijn).



Figuur 48: Totaaloverzicht niveaumetingen RWZI Scheve Klap

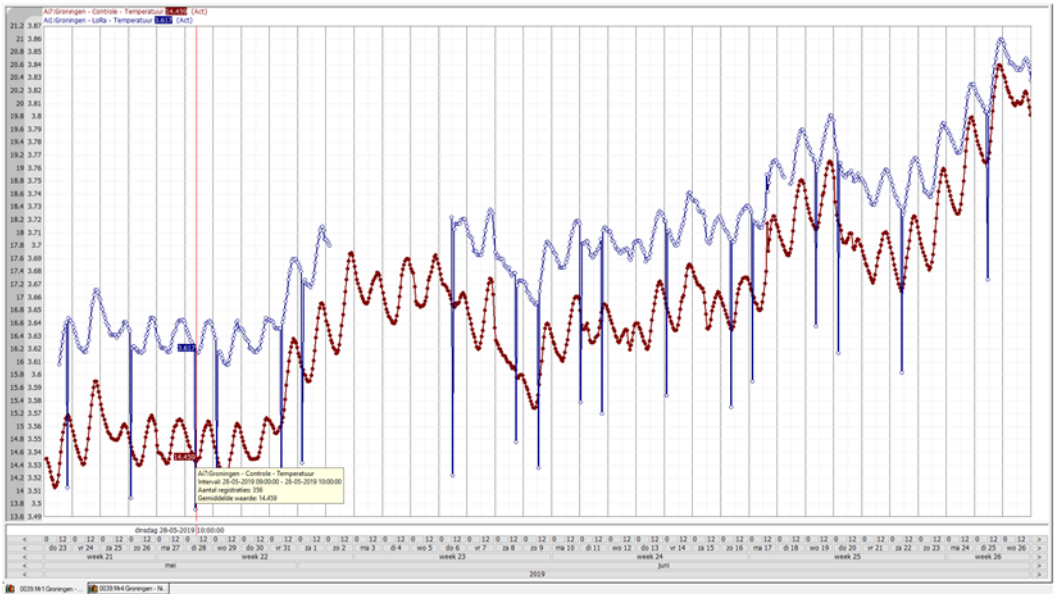


Figuur 49: Weekoverzicht niveaumetingen RWZI Scheve Klap

Het trendverloop van de data is in het algemeen goed te noemen. Het iets uit de pas lopen van de metingen kan mogelijk verklaard worden door verschil in meettijdstippen en verschil in meetinterval.

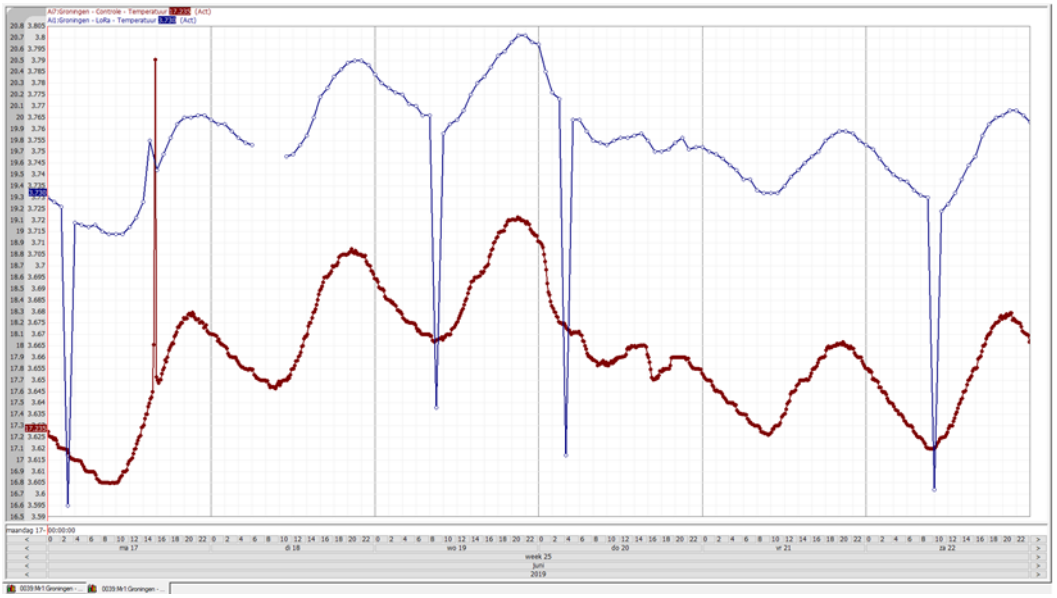
5.3.6 RWZI Scheve Klap temperatuur-meting

In Figuur 50 is een overzicht te zien van de data met betrekking tot de temperatuurmetingen in de periode van 24 mei t/m 26 juni en in Figuur 51 een overzicht van de data in de periode 17 t/m 22 juni. De blauwe lijn geeft de gemeten waarde weer zoals gemeten met de proefopstelling met de LoRa node. De rode lijn geeft de gemeten waarden weer die ter beschikking zijn gesteld door het waterschap.



Figuur 50: Totaaloverzicht temperatuurmetingen RWZI Scheve Klap

Ook hier is goed de storing te zien in de periode van 4 t/m 6 juni waar data van de LoRa node ontbreekt (blauwe lijn).



Figuur 51: Weekoverzicht temperatuurmetingen RWZI Scheve Klap

Het trendverloop van beide grafieken komt heel mooi overeen. Opvallend is wel dat er in de LoRa data (blauwe lijn) wederom uitschieters naar beneden zichtbaar zijn. Voor deze “tranen” hebben we geen duidelijke oorzaak kunnen vinden. Mogelijk geeft de sensor een verkeerde waarde en wordt deze door de LoRa node incorrect geïnterpreteerd. Een andere mogelijkheid is dat een error-waarde voor een meting wordt aangezien.

5.4 Overzicht van de meetresultaten

Tabel 5 geeft een overzicht van de ontvangen meetwaarden ten opzichte van het te verwachten aantal meetwaarden. Dit betreft de hele periode inclusief storingen en inclusief de aanloopperiode voor Chaam en Heeswijk. Voor Chaam en Heeswijk is een periode van 34 dagen gemeten (van 24 mei 2019 t/m 26 juni 2019) wat overeenkomt met 34 x 24 = 816 metingen. De opstelling in Scheve Klap heeft geen aanloopperiode gehad en hier is een periode van 30 dagen gemeten (van 1 juni 2019 t/m 30 juni 2019) wat overeenkomt met 30 x 24 = 720 metingen voor de niveau-sensor en 30 x 24 x 30 = 21600 metingen voor de temperatuur-sensor.

Locatie	Soort meting	Verwacht aantal	Gemeten aantal	Gemist aantal	Percentage ontvangen
RWZI Chaam	Niveau	816	758	56	92,89%
RWZI Chaam	Kwaliteit	816	752	64	92,15%
RWZI Heeswijk Dinther	Niveau	816	753	62	92,27%
RWZI Heeswijk Dinther	Kwaliteit	816	739	77	90,56%
RWZI Scheve Klap	Niveau	720	599	121	83,19%
RWZI Scheve Klap	Temperatuur	21600	17004	4596	78,72%

Tabel 5: Overzicht van alle ontvangen meetwaarden (storingsdagen meegerekend)

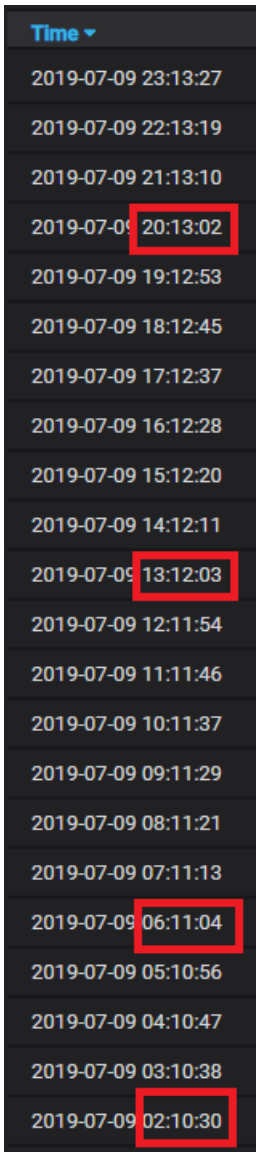
De storingen in zowel Chaam en Heeswijk als die in Scheve Klap kunnen niet aangerekend worden aan LoRa want dit zijn geen LoRa problemen. Als we de storingsdagen eruit filteren en alleen storingsvrije dagen meetellen, dan ontstaat het beeld zoals weergegeven in Tabel 6.

Locatie	Soort meting	Verwacht aantal	Gemeten aantal	Gemist aantal	Percentage ontvangen
RWZI Chaam	Niveau	768	758	8	98,69%
RWZI Chaam	Kwaliteit	768	752	16	97,91%
RWZI Heeswijk Dinther	Niveau	768	753	15	98,04%
RWZI Heeswijk Dinther	Kwaliteit	768	739	29	96,22%
RWZI Scheve Klap	Niveau	528	515	13	97,53%
RWZI Scheve Klap	Temperatuur	15840	14718	1122	92,91%

Tabel 6: Overzicht van alle ontvangen meetwaarden (storingsdagen niet meegerekend)

Voor Chaam en Heeswijk zijn er in totaal twee storingsdagen geweest. Als we deze van het totaal aantal dagen afhalen, houden we 34 - 2 = 32 storingsvrije dagen over. Dit komt overeen met 32 x 24 = 768 metingen. Voor Scheve Klap zijn er in totaal zes storingsdagen geweest (de 1^{e} dag is niet volledig geweest en kunnen we daarom niet meetellen). Omdat Scheve Klap ook nog een deel in juli 2019 actief is geweest, zoeken we ook hier naar zoveel mogelijk storingsvrije dagen. Dit is de periode 19 juni 2019 t/m 10 juli 2019 voor een totaal van 22 dagen. Dit komt overeen met 22 x 24 = 528 te verwachten metingen voor de niveau-sensor en 22 x 24 x 30 = 15840 te verwachten metingen voor de temperatuur-sensor.

Bij bovenstaande berekeningen en percentages moet direct een kanttekening gemaakt worden. Namelijk dat we niet zomaar mogen aannemen dat een 1-uur-sensor ook daadwerkelijk 24 metingen per etmaal heeft geprobeerd te versturen en een 2-minuten-sensor 24 x 30 = 720 metingen per etmaal.



Figuur 52: Tijdstip van ontvangen metingen voor Scheve Klap

In Figuur 52 is te zien dat de tijdstippen van de ontvangen berichten telkens een beetje opschuiven in de tijd. Met andere woorden misschien heeft de sensor-node over een langere periode een ander aantal sensorberichten geprobeerd te versturen dan aangenomen. Dit is afhankelijk van hoe de LoRa-nodes zijn geprogrammeerd. Om correct te kunnen berekenen hoeveel sensorberichten goed zijn aangekomen, zou ook op de sensor-node bijgehouden moeten worden hoeveel berichten de sensor-node heeft geprobeerd te versturen. Daarom moeten de berekeningen en de percentages gezien worden als een ‘best-effort’ benadering.

5.5 Analyse van de resultaten van Applied Risk (privaat LoRa)

Applied Risk heeft drie van de vijf scenario's kunnen ontwikkelen en uitproberen op de proefopstelling (zie Figuur 53).

Attack	Possible	Tested	Comments
Bit flipping attacks	Yes	No	Server-to-server traffic was observed, and it showed that integrity checking was stripped. This did not require testing, since it's a known property of the underlaying cryptographic mechanism that this attack is possible.
Replay attack	Yes	Yes	Replay attacks could be demonstrated but can be mitigated with the right settings and the right implementation.
Perform OTAA related attacks	No	Yes	Attacks on the OTAA implementation – such as replay attacks - have been performed but did not lead to hijacking or decryption of data traffic.
Attacks on public interfaces	Unknown	No	No public interfaces were available during testing.
Re-provisioning of previously used encryption keys	Yes	Yes	If an attacker knows the AppKey - which is the main encryption key - for a device, it allows for data manipulation, connection hijacking and data decryption.

Figuur 53: Resultaten Applied Risk (Bron: [4])

Figuur 54: LoRa Technology Evaluation Kit

Hierbij is gebruik gemaakt van een LoRa Technology Evaluation Kit (zie Figuur 54). Daarnaast is door Applied Risk software ontwikkeld om 'reverse engineering' te kunnen doen.

5.5.1 OTAA Activation Attacks

Voor wat betreft de OTAA aanvallen kunnen we kort zijn. Die zijn uitgeprobeerd maar niet gelukt.

5.5.2 Replay Attacks

De replay aanval is wel gelukt. Door LoRa traffic op te nemen en weer uit te zenden kan onze visualisatie applicatie (Grafana) voor de gek worden gehouden (zie Figuur 55). Aan de rechterkant van de figuur is zogenaamd een ‘dip’ te zien in de metingen maar dit zijn oude LoRa berichten met daarin lage meetwaarden die opnieuw worden uitgezonden. Met andere woorden de metingen zijn volledig integer en authentiek, ze zijn alleen verouderd. In werkelijkheid hadden de metingen in de grafiek netjes door moeten lopen.

Figuur 55: Replay aanval

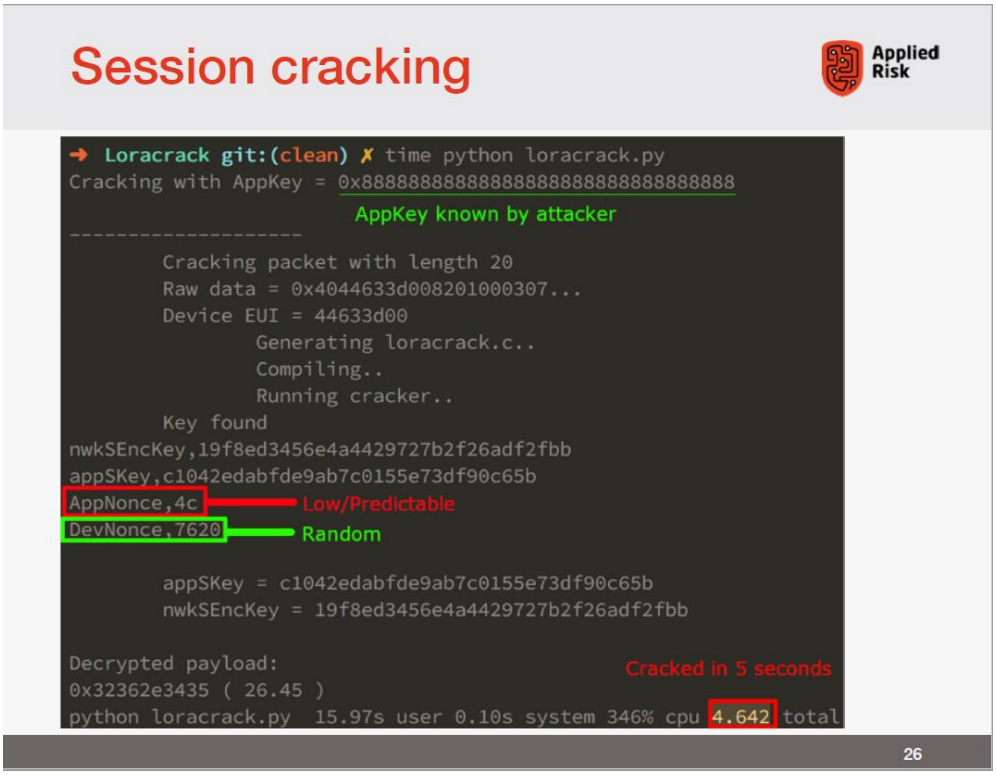
Dit heeft te maken met het Frame Counter beveiligingsmechanisme in de LoRaServer software. Deze kan namelijk met een vinkje in de managementinterface aan- en uitgeschakeld worden (zie Figuur 56).

Figuur 56: LoRaServer management interface

In de begeleidende tekst valt te lezen: “*Note that disabling the frame-counter validation will compromise security as it enables people to perform replay-attacks*”. Het is daarmee bewezen dat dit beveiligingsmechanisme belangrijk is en aan moet staan (staat standaard aan).

5.5.3 AppKey Attack

De meest interessante aanval van Applied Risk is de “session cracking” aanval (zie Figuur 57). Dit is het scenario waarbij een aanvaller de beschikking krijgt over de AppKey, bijvoorbeeld doordat deze AppKey uit een sensor kan worden geëxtraheerd. Om dit scenario wat sneller en makkelijker te kunnen uitvoeren, hebben we Applied Risk de AppKey gegeven die was geconfigureerd in één van de test-sensoren.

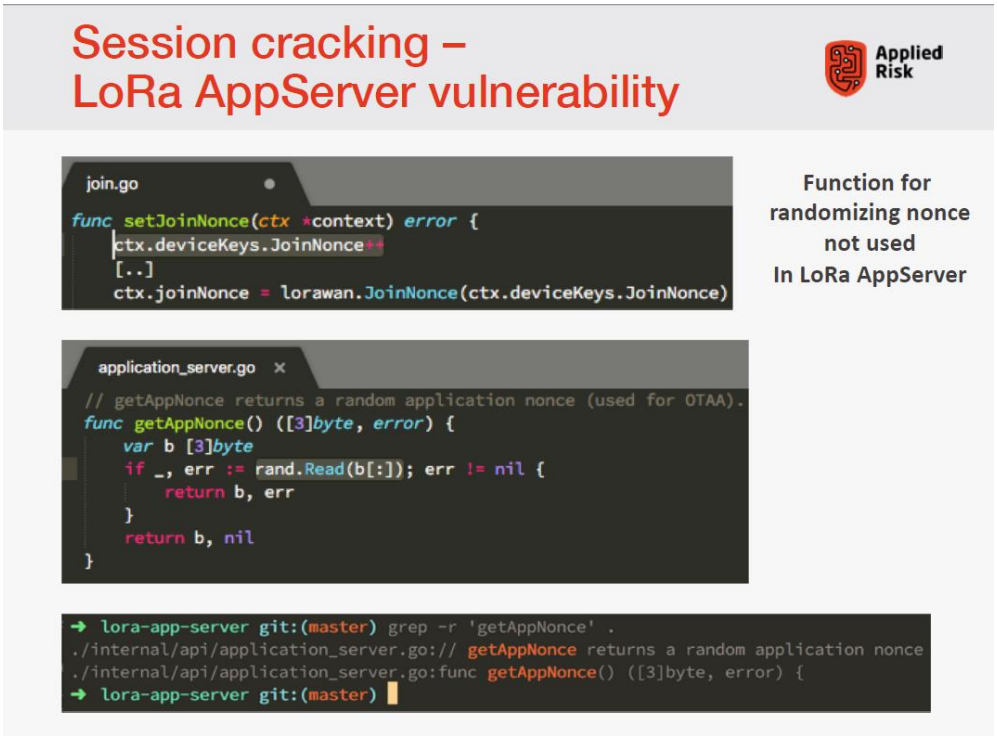


Figuur 57: Session cracking

Met alleen deze AppKey konden de mensen van Applied Risk met eigen software en hardware in 4.6 seconden LoRa berichten uit de lucht opvangen en de payload decrypten. De afgeluisterde meting betreft een temperatuurmeting van 26.45 graden Celsius. Het is daarmee bewezen dat de AppKey erg belangrijk is en geheim moet worden gehouden.

Daarbij moet opgemerkt worden dat de ‘nonces’ in de LoRaServer software niet random bleken te zijn (zie Figuur 58), zoals wordt voorgeschreven in de specificatie[26], terwijl er wel een functie voor geïmplementeerd was in de software.

[26] Zie LoRaWAN Specification v1.0.2 in paragraaf 6.2.4 op pagina 34 (‘DevNonce’) en paragraaf 6.2.5 op pagina 35 (‘AppNonce’)



Figuur 58: Functie voor randomizing nonce

In de meest recente versie van de LoRaServer software (zie Figuur 59) is de implementatie van de ‘setJoinNonce’ functie aangepast[27].

```
109  func setJoinNonce(ctx *context) error {
110          if ctx.deviceKeys.JoinNonce > (1<<24)-1 {
111                  return errors.New("join-nonce overflow")
112          }
113          ctx.joinNonce = lorawan.JoinNonce(ctx.deviceKeys.JoinNonce)
114          return nil
115  }
116
```

Figuur 59: setJoinNonce (Bron: GitHub)

Daarnaast schrijft de specificatie voor dat elke sensor met een unieke ‘gepersonaliseerde’ AppKey moet worden uitgerust (‘key diversification’)[28].

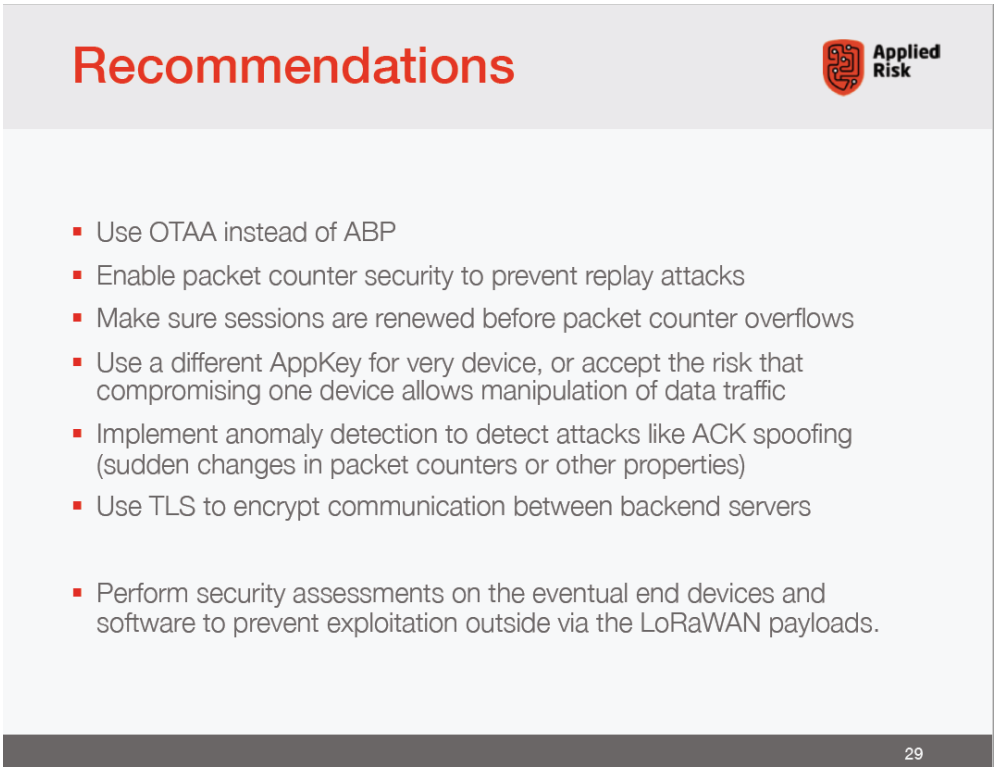
[27] Zie https://github.com/brocaar/lorawan/blob/master/backend/joinserver/join_request.go
[28] Zie LoRaWAN Specification v1.0.2 in paragraaf 6.2.2 op pagina 33

Attack	Possible	Tested	Comments
Bit flipping attacks	Yes	No	Server-to-server traffic was observed, and it showed that integrity checking was stripped. This did not require testing, since it's a known property of the underlaying cryptographic mechanism that this attack is possible.
Replay attack	Yes	Yes	Replay attacks could be demonstrated but can be mitigated with the right settings and the right implementation.
Perform OTAA related attacks	No	Yes	Attacks on the OTAA implementation – such as replay attacks - have been performed but did not lead to hijacking or decryption of data traffic.
Attacks on public interfaces	Unknown	No	No public interfaces were available during testing.
Re-provisioning of previously used encryption keys	Yes	Yes	If an attacker knows the AppKey - which is the main encryption key - for a device, it allows for data manipulation, connection hijacking and data decryption.

Figuur 60: Samenvatting resultaten

Samenvattend (zie Figuur 60) kunnen we stellen dat:

- Er geen problemen zijn gevonden met de OTAA procedure (Groen).
- Er wel problemen zijn gevonden met replay aanvallen. Maar dit is makkelijk te verhelpen door het Frame Counter beveiligingsmechanisme aan te zetten (Oranje).
- De AppKey van elke sensor geheim moet worden gehouden. Als deze uitlekt, ontstaan problemen (Rood).



Figuur 61: Aanbevelingen

Applied Risk heeft de volgende aanbevelingen gedaan (zie Figuur 61). Voor meer details en achtergrondinformatie van de onderzoeksresultaten van Applied Risk zie [4, 5].

6 Evaluatie

Op basis van de onderzoeksresultaten zijn we tot de volgende bevindingen gekomen met betrekking tot de onderzoeksvragen:

(1) Voldoet LoRaWAN aan de minimale set van eisen om te kunnen worden gebruikt in een nieuwe generatie van watertoepassingen?

1. LoRaWAN voldoet functioneel gezien aan de minimale set van eisen (ID1-ID7) om te kunnen worden gebruikt in een nieuwe generatie van watertoepassingen. We baseren deze conclusie op het feit dat van de met deze technologie verzonden sensorberichten (voor zes proefopstellingen verspreid over drie locaties in Nederland) minimaal 92,91% van de verstuurde sensorberichten goed zijn ontvangen voor het private LoRa netwerk en minimaal 96,22% voor het KPN LoRa netwerk. Op basis van deze meetwaarden ontstaat een beeld dat dicht genoeg tegen de contra-metingen aan zit van de waterschappen zelf.

2. Uitzondering hierop is het updaten van firmware (ID6). Dit aspect staat wel opgenomen in de eisen maar is niet in de praktijk uitgeprobeerd. Dat wil overigens niet zeggen dat het niet mogelijk is.

3. Het is opvallend dat er in de LoRa grafieken uitschieters naar beneden zichtbaar zijn (zie Figuur 35, Figuur 43, Figuur 50 en Figuur 51) terwijl deze niet zichtbaar zijn in de grafieken van de contra-metingen. Dit ligt niet aan de LoRa technologie zelf maar aan de integratie van de industriële sensor en de ITALKS MCS 1608 LoRa-node. Wellicht dat voor het oplossen van deze “tranen” meerdere iteraties nodig zijn om deze apparaten beter te laten samenwerken.

(2) Is het mogelijk om op een reproduceerbare manier aannemelijk te maken dat LoRaWAN veilig dan wel niet veilig genoeg is om te kunnen worden geadopteerd door de waterschappen in een nieuwe generatie van watertoepassingen?

4. Het oorspronkelijke idee van een geautomatiseerd security test-framework met daarin allerlei security test-cases van meerdere beveiligingsbedrijven binnen een Nationaal Cybersecurity Testbed (zie Bijlage A) bleek niet realiseerbaar binnen dit project. Onder andere omdat het security analyse werk veelal uit handwerk bestaat maar ook omdat het concept niet haalbaar was binnen de scope en het budget van dit project. In dit project hebben we wel een eerste stap gezet door drie security test-scenario’s op een proefopstelling uit te proberen.

5. Applied Risk heeft drie security scenario’s ontwikkeld en uitgevoerd. Deze scenario’s zijn uitgeprobeerd op het private LoRa netwerk. De belangrijkste conclusie die kan worden gebaseerd op hun bijdrage, is dat het kritisch is om de AppKey geheim te houden. Hun onderzoek heeft aangetoond dat een zorgvuldige inrichting van ‘key management’ van belang is (zie par.

5.5). Daarnaast is gebleken dat het ook belangrijk is om een software implementatie te gebruiken die de specificatie goed implementeert.

6. Naast de al aanwezige beveiligingsfeatures in LoRaWAN, hebben we binnen dit project ervaring opgedaan met het gebruik van sleutelopslag in een Secure Element om zo een extra beveiligingslaag toe te voegen met betrekking tot Integriteit en Vertrouwelijkheid (zie Bijlage B).

7. Om inzicht te geven in hoe KPN hun LoRaWAN IoT netwerk geschikt heeft gemaakt voor het E2E transporteren van sensordata, heeft KPN een beschrijving van de geïmplementeerde maatregelen in hun LoRaWAN netwerk bijgevoegd (zie Bijlage C).

7 Referenties

1. TNO, TKI HTSM Projectvoorstel "*Beveiliging watermanagement naar een hoger peil met IoT*" (versie 1.1), 8 september 2017
2. EW-Installatietechniek, "*Waterschappen duiken in Internet of Things*", David van Baarle, Juli/Augustus 2018, beschikbaar op https://www.tmx.nl/wp-content/uploads/2018/10/Artikel-EW-installatietechniek-aug-2018.pdf
3. TU Delft, "*LoRaWAN: Vulnerability Analysis and Practical Expoitation*", Yang Xueying, 2017, beschikbaar op https://repository.tudelft.nl/islandora/object/uuid%3A87730790-6166-4424-9d82-8fe815733f1e
4. Applied Risk, "*Final Report Beveiliging watermanagement naar een hoger peil met IoT, Security testing LoRaWAN 1.0 Protocol*", Sipke Mellema, Scott Thomas, Tom Westenberg, Jalal Bouhdada, 28 March 2019
5. Applied Risk, "*20180901-TNO-TKI-RSRCH Research results*", March 28, 2019

8 Bijlage A – Nationaal Cybersecurity Testbed

In 2015 bezocht een Nederlandse politieke- en handelsmissie[29] Japan, waar onder kennis werd gemaakt met een onderdeel van de Japanse aanpak van Cyberveiligheid: het Control System Security Center (CSSC). Dit CSSC biedt onder andere een multi-sectoraal testbed[30] waarin kritische infrastructuren voor Japan getest worden op veiligheid. Een gelijksoortige aanpak zou ook voor Nederland van toegevoegde waarde kunnen zijn. Want toenemend gebruik van de cyberinfrastructuur, ook voor maatschappelijk kritische processen, kan leiden tot een grotere complexiteit, afhankelijkheid en daarmee grotere risico's voor de maatschappij.

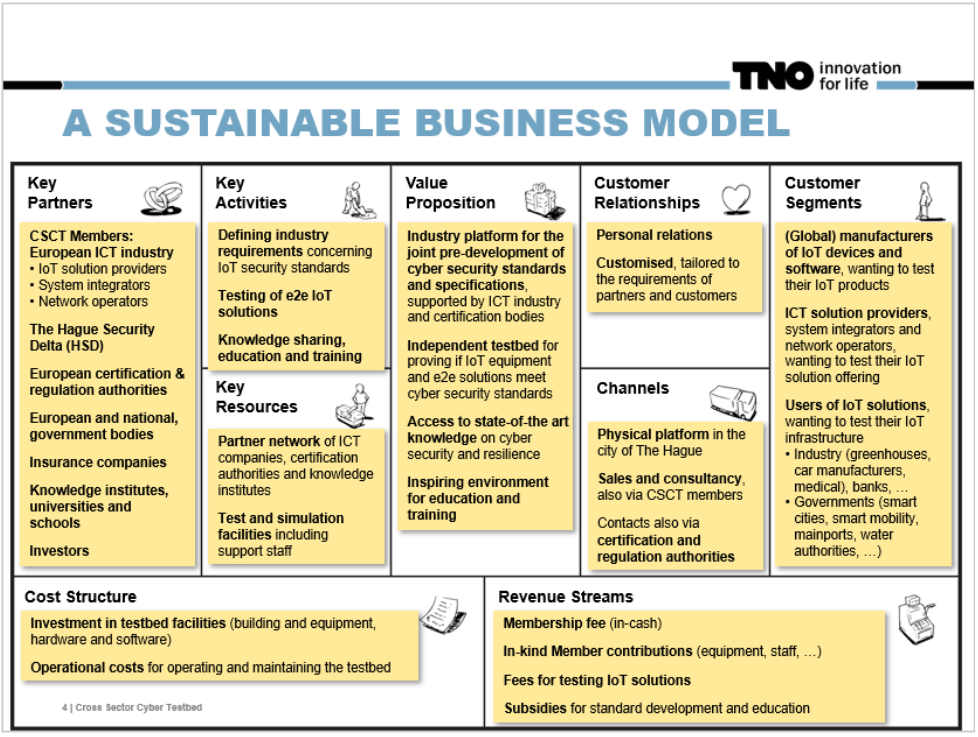
Figuur 62: Cyber testbed vision

In een dergelijke omgeving zouden partijen met security kennis en skills nieuwe producten of technologieën kunnen uitproberen en op zoek gaan naar zwakke plekken. En wanneer zwakke plekken gevonden worden, kunnen deze onder gecontroleerde omstandigheden worden gedemonstreerd. Om daarna een technologie vendor of een andere partij in staat te stellen de zwakke plek te verhelpen middels het doorvoeren van verbeteringen.

In TNO's visie zou in een dergelijke omgeving op basis van een 'Automated Security' methodiek een security test-framework[31] aangeboden moeten worden

[29] Zie https://denhaag.raadsinformatie.nl/document/3351557/1/RIS290066 Reisverslag handelsmissie Japan
[30] Zie https://www.isasecure.org/en-US/Documents/Articles-and-Technical-Papers/201403about_CSSC_ppt_en-pdf-(1)
[31] Bijvoorbeeld op basis van https://learn.chef.io/modules/try-inspec/ of https://github.com/nintexplatform/sentinel

waarmee veelgemaakte protocolfouten, cryptografiefouten, software fouten, state-machine fouten enzovoort herhaaldelijk, geautomatiseerd en transparant moeten kunnen worden uitgevoerd. Een dergelijk security test-framework zou ook makkelijk moeten kunnen worden uitgebreid door verschillende partijen zodat een Automated Security Test Suite van wereldklasse kan ontstaan.



Figuur 63: Cyber testbed business model

Hierbij is het cruciaal dat zoveel mogelijk security experts toegang krijgen tot zo'n omgeving om een zo goed mogelijke 'coverage' te krijgen[32]. Denk hierbij aan IT beveiligingsbedrijven zoals Applied Risk, Fox-IT en HackerOne. Maar ook aan security vakgroepen van universiteiten met hoogleraren, promovendi en studenten. En aan de experts bij het Nationaal Cyber Security Centrum (NCSC) en KPN Security. Maar ook aan individuele hackers die in zo'n proefopstelling een enorme uitdaging zien maar niet verbonden (willen) zijn aan een bedrijf of instelling.

[32] Linus's Law is a claim that states "given enough eyeballs, all bugs are shallow", zie https://en.wikipedia.org/wiki/Linus%27s_Law

9 Bijlage B – Implementing a third layer of security

9.1 Secure Element

Sodaq verkoopt een sensor-bord onder de naam Sodaq Explorer[33] met een zogenaamd Secure Element[34] (zie Figuur 64). Een Secure Element is een aparte security chip, in dit geval de Microchip ATECC508A[35], die conceptueel vergelijkbaar is met bijvoorbeeld een smartcard of een SIM kaart. De belofte van een Secure Element is dat cryptografische sleutels die erop staan er niet afgehaald kunnen worden, ook al heeft een aanvaller langdurig fysieke beschikking over de chip.

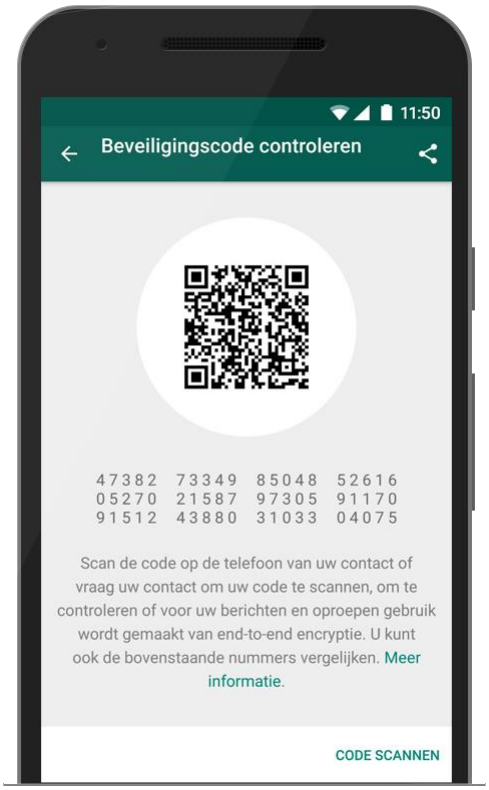
Figuur 64: Sodaq Explorer

Voor het beveiligen van LoRaWAN 'in-transit' communicatie over de hele sensorketen heen (End-to-End Encryption[36]) heeft Jan Willem Smeenk van Sodaq een interessant filmpje op Youtube[37] staan getiteld "Implementing a third layer of security".

Je kunt als gebruiker van een LoRaWAN netwerk ervoor kiezen om te vertrouwen op de security features die in de netwerktechnologie zitten. Als dit om welke reden dan ook niet voldoende is voor een bepaalde toepassing, kun je kijken hoever je kunt komen met het zwaarder beveiligen van de sensorketen door er een extra laag van beveiliging overheen te leggen. Hiermee wordt het mogelijk om over de LoRaWAN verbinding heen extra beveiligingsmaatregelen te implementeren voor het beschermen van Integriteit en Vertrouwelijkheid uit het CIA model[38]. De crux hiervan is dat dan alleen de sensor en de klantapplicatie toegang hebben tot het sleutelmateriaal. Daarnaast kan op deze manier flexibel gekozen worden voor bepaalde encryptiealgoritmes in combinatie met grotere 'key size'[39].

---

[33] Zie https://support.sodaq.com/sodaq-one/explorer/
[34] Zie https://www.justaskgemalto.com/en/what-is-a-secure-element/
[35] Zie https://www.microchip.com/wwwproducts/en/ATECC508A
[36] Zie https://en.wikipedia.org/wiki/End-to-end_encryption
[37] Zie https://www.youtube.com/watch?v=6Jv6PB46Lqo
[38] Zie https://en.wikipedia.org/wiki/Information_security
[39] Zie https://en.wikipedia.org/wiki/Key_size



Figuur 65: WhatsApp end-to-end encryptie

Vergelijk het met de end-to-end encryptie van WhatsApp (zie Figuur 65). WhatsApp zegt dat hun communicatie end-to-end beveiligd is maar hun applicatie is closed-source dus we kunnen het niet controleren. Misschien kunnen ze voor bepaalde gebruikers de beveiliging wel even uit zetten. Of een encryptiesleutel genereren die niet random is. Met andere woorden de gebruikers van WhatsApp moeten vertrouwen op de technologie die WhatsApp biedt en dat kan voor bepaalde toepassingen afdoende zijn.

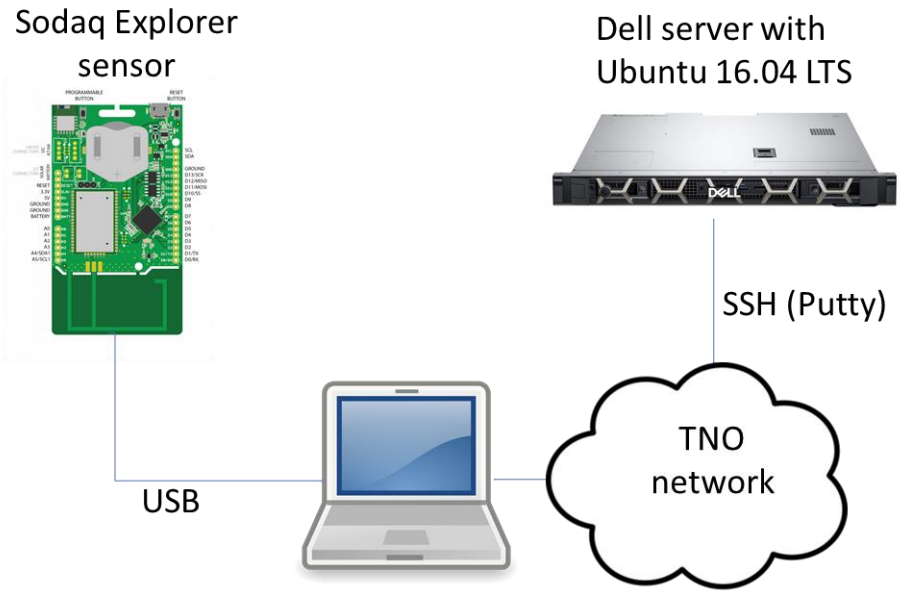
Als dat niet afdoende is en je meer ‘in-control’ wilt zijn van je risico’s en je maatregelen kun je ook een extra encryptie applicatie installeren op je telefoon. Hiermee kun je een plaintext bericht bestemd voor een vriend eerst vercijferen en daarna de ciphertext in WhatsApp copy/pasten en versturen.

Dit heeft de volgende voordelen:

1. Je kunt zelf kiezen voor bepaalde encryptiealgoritmes en/of langere sleutels.
2. Het sleutelmateriaal is alleen bekend bij zender en ontvanger.
3. Je hoeft voor wat betreft Integriteit en Vertrouwelijkheid van de berichten niet te vertrouwen op WhatsApp (wel op de extra encryptie applicatie) want WhatsApp doet alleen het transport.
4. WhatsApp zelf kan niet bij de inhoud van het bericht komen.

9.2 Testopstelling

We hebben een kleine testopstelling gemaakt rondom de Sodaq Explorer om dit concept uit te proberen (zie Figuur 66).



Figuur 66: Opstelling Sodaq Explorer

Op de laptop gebruiken we de Arduino IDE om de Sodaq Explorer te programmeren. Via Secure Shell (SSH) is de laptop ook verbonden met een server in het sensorlab van TNO en op deze server is OpenSSL[40] beschikbaar. OpenSSL is te gebruiken als een 'Zwitsers zakmes' voor cryptografie. Via de input en output van de Arduino IDE en de SSH sessie kunnen we encryptie-experimenten uitvoeren door plaintext en ciphertext te copy / pasten tussen beide omgevingen.

Het doel van deze opstelling is om te kijken hoe een extra laag van beveiliging bovenop LoRaWAN zou kunnen werken met de Sodaq Explorer Secure Element.

9.3 Elliptic-Curve Diffie–Hellman

We willen een standaard library als OpenSSL kunnen laten samenwerken met de Sodaq Explorer ATECC508A crypto chip en dat volledig buiten de features van LoRaWAN om. Hoe ziet zo'n proces er globaal uit?

Op het Sodaq Support Forum hebben we de Explorer_Crypto[41] library gevonden. Deze library blijkt ondersteuning te hebben voor het zogenaamde 'Elliptic-Curve Diffie–Hellman[42]' (ECDH) algoritme. Op basis van dit algoritme kunnen twee partijen zoals bijvoorbeeld een sensor-node en een klant-applicatie gezamenlijk maar onafhankelijk van elkaar een encryptiesleutel afspreken. Op deze manier gaat er niks over de lijn waar een aanvaller misbruik van zou kunnen maken.
Het globale ECDH proces op basis van alleen OpenSSL kan worden uitgeprobeerd met de volgende stappen[43].

[40] Zie https://en.wikipedia.org/wiki/OpenSSL
[41] Zie https//github.com/GabrielNotman/ExpLoRer_Crypto
[42] Zie https://en.wikipedia.org/wiki/Elliptic-curve_Diffie%E2%80%93Hellman
[43] Zie https://jameshfisher.com/2017/04/14/openssl-ecc.html

(1) Alice en Bob genereren met OpenSSL beide een asymmetrisch sleutelpaar (een private key en een public key).

```
# Alice generates her keypair
$ openssl ecparam -name secp256k1 -genkey -noout -out
alice_priv_key.pem
# Alice extracts her public key from her private key
$ openssl ec -in alice_priv_key.pem -pubout -out
alice_pub_key.pem
```

```
# Bob generates his keypair
$ openssl ecparam -name secp256k1 -genkey -noout -out
bob_priv_key.pem
# Bob extracts his public key from his private key
$ openssl ec -in bob_priv_key.pem -pubout -out
bob_pub_key.pem
```

(2) Alice en Bob genereren beide een shared-secret op basis van de eigen private key en de public key van de ander.

```
# Bob and Alice generate their shared secret
$ openssl pkeyutl -derive -inkey alice_priv_key.pem -peerkey
bob_pub_key.pem -out alice_shared_secret.bin
$ openssl pkeyutl -derive -inkey bob_priv_key.pem -peerkey
alice_pub_key.pem -out bob_shared_secret.bin
$ base64 alice_shared_secret.bin
uAt0erghSSRluSk1v+y8kGo6eMekR9ORVRNf22vLYbA=
$ base64 bob_shared_secret.bin
uAt0erghSSRluSk1v+y8kGo6eMekR9ORVRNf22vLYbA=
```

(3) Alice kan nu een plaintext vercijferen en de ciphertext naar Bob sturen en Bob kan de ciphertext ontcijferen.

```
$ echo 'I love Belgian beer' > plain.txt
$ openssl enc -aes256 -base64 -k $(base64
alice_shared_secret.bin) -e -in plain.txt -out cipher.txt
$ cat cipher.txt
U2FsdGVkX18V95us9J3WKjQrw12cx0EJF+7MiuB7ebzwykPLydeVeItz71Cqy
qBf
```

```
$ openssl enc -aes256 -base64 -k $(base64
bob_shared_secret.bin) -d -in cipher.txt -out plain_again.txt
$ cat plain_again.txt
I love Belgian beer
```

9.4 OpenSSL

Nu willen we bovenstaande stappen combineren met de Sodaq Explorer Secure Element. Op de Sodaq Explorer kan een keypair worden gegenereerd op ATECC508A crypto chip voor het ECDH algoritme met de volgende source-code.

```
  //Generate private key in slot 2
  uint8_t pub_key_slot2[ATCA_PUB_KEY_SIZE];
  debugSerial.print("Generating private key in slot2:...");
  showResult(atcab_genkey(2, pub_key_slot2));
  debugSerial.println("Responded with public key:");
  printHex(pub_key_slot2, sizeof(pub_key_slot2), 16);
  debugSerial.println();
```

Daarna kan de public key behorende bij de private key in slot 2 worden opgevraagd.

```
  //Query public key of slot 2
  debugSerial.print("Querying public key from secret key in
slot2:...");
  showResult(atcab_get_pubkey(2, pub_key_slot2));
  printRawHex(pub_key_slot2, sizeof(pub_key_slot2));
  debugSerial.println();
```

Nadat de public key van de server ingevoerd is in de Arduino Serial Monitor, kan de Sodaq een shared secret genereren.

```
  //Generate shared secret 2 -> external
  uint8_t shared_sec[ATCA_KEY_SIZE];
  memset(shared_sec, 0, sizeof(shared_sec));
  debugSerial.print("Generating shared secret 2-
>external:...");
  showResult(atcab_ecdh(2, pub_key_ext, shared_sec));
  printRawHex(shared_sec, sizeof(shared_sec));
  debugSerial.println();
```

Op de Arduino Serial Monitor is dan de volgende uitvoer te zien.

```
Querying public key from secret key in slot2:...SUCCESS
6A0DB9C057F5C5F83A316FFF28078002268366A3F81048B4B2734BAAFD7FE
A7383F70587339347AA4DC6B1E5016F952CEF3C716ED3BA69C6ED021EA13B
FA2023


Enter an external public key:
Received:
```

```
3093CDCF637BAB3E84A41B6959F798727739BC76715B65D231CE203A7E907
15D257E0FEA28CCA5AF74DE5920583363F7F8B4C811D1B330E701DC2AFC22
AFC048


Generating shared secret 2->external:...SUCCESS
FC85B58A080814505FA9C48F0A222D458E1DC3D4524B75B2D921EBC0C9C4C
82D
```

Op de server doen we hetzelfde en controleren of de gegenereerde shared secret overeen komt met die op de Sodaq. Daarna vercijferen we een plaintext op de Sodaq.

```
  //TRNG test
  uint8_t random_num[32];
  debugSerial.print("Requesting TRNG:...");
  showResult(atcab_random(random_num));
  printHex(random_num, sizeof(random_num), 16);
  debugSerial.println();

  //Run AES-CBC encrypt test
  char* messageCBC = "Test using AES-256 Cipher Block
Chaining encryption";
  messageLen = strlen(messageCBC);
  blocks = (messageLen / AES_BLOCKLEN) + 1; // No pad option
+ (messageLen % AES_BLOCKLEN ? 1 : 0);
  uint8_t cipherCBC[blocks * AES_BLOCKLEN];
  memcpy(cipherCBC, messageCBC, sizeof(cipherCBC));
  cipherCBC[messageLen] = 0;

  debugSerial.println("AES-256-CBC encryption test");
  debugSerial.print("Plain text: ");
  debugSerial.println(messageCBC);

  debugSerial.print("Adding PKCS7 padding:...");
  padBytes = pkcs7_padding_pad_buffer(cipherCBC, messageLen,
sizeof(cipherCBC), AES_BLOCKLEN);
  debugSerial.println((padBytes == 0 ? "FAIL" :
(String("SUCCESS ") + String(padBytes, DEC))));

  //Encrypt using TRNG data for IV
  uint8_t iv[AES_BLOCKLEN];
  memcpy(iv, random_num, sizeof(iv));

  AES_init_ctx_iv(&ctx, shared_sec, iv);
  AES_CBC_encrypt_buffer(&ctx, cipherCBC, sizeof(cipherCBC));

  debugSerial.print("IV:");
  printRawHex(iv, sizeof(iv));
  debugSerial.println("Cipher text:");
  printRawHex(cipherCBC, sizeof(cipherCBC));
  debugSerial.println();
```

Op de Arduino Serial Monitor is dan de volgende uitvoer te zien.

```
AES-256-CBC encryption test
Plain text: Test using AES-256 Cipher Block Chaining
encryption
Adding PKCS7 padding:...SUCCESS 13
IV:1CB17766B37583DFDA4C2B4D038A2AEB
Cipher text:
C420A4CC5E7770BCC1B18FB1B9A605B07769D6801D4F53E91883FBBD957CB
233915099E6C65390CEF927F909B24C75308ED736DF1CA0EBD7A6CAA4472F
5B1D69
```

En vervolgens proberen we de ciphertext op de server te ontcijferen met OpenSSL.

```
$ vim ciphertext.hex
$ xxd -r -p ciphertext.hex ciphertext.bin
$ openssl enc -aes-256-cbc -K
FC85B58A080814505FA9C48F0A222D458E1DC3D4524B75B2D921EBC0C9C4C
82D -iv 1CB17766B37583DFDA4C2B4D038A2AEB -d -in
ciphertext.bin -out plain_again.txt
$ cat plain_again.txt
Test using AES-256 Cipher Block Chaining encryption
```

Daarmee is aangetoond dat de Sodaq Explorer data kan vercijferen[44] met behulp van een door ECDH-algoritme gegenereerde encryptiesleutel op basis van een geheime sleutel die in de Secure Element staat opgeslagen. Ook is bewezen dat de resulterende ciphertext met behulp van een andere software-suite (OpenSSL) deze data kan ontcijferen.

[44] Merk op dat dit experiment alleen extra encryptie doet (Vertrouwelijkheid) en nog geen extra Integriteit.

10 Bijlage C – Security in KPN LoRaWan network

During this project two networks were used to test: a private LoRa setup and KPN's public LoRa network. On the KPN LoRa WAN-network KPN's own security mechanisms are applicable. The complete solution is hosted in KPN-owned data centres where the KPN Security Policy (KSP) is applicable. The KSP is rule-based and consists of OWASP, NIST and parts of ISO learning from the Industry like security (ISO27001[45]) and the international standard for business continuity (BS25999). The KPN LoRa network is also compliant with the "Baseline Informatiebeveiliging Rijksdienst (BIR)" which allows KPN LoRa network to be used within the Netherlands by the "Ministerie van Infrastructuur en Waterstaat" (IenW).

This Appendix describes how KPN, if applicable, deals with the recommendations done by Applied Risk. The most important conclusion in this is that the vulnerabilities as discovered by Applied Risk in the private network, were already foreseen by KPN and thus implemented in the KSP. The KSP makes sure these vulnerabilities do not exist in KPN's public network.

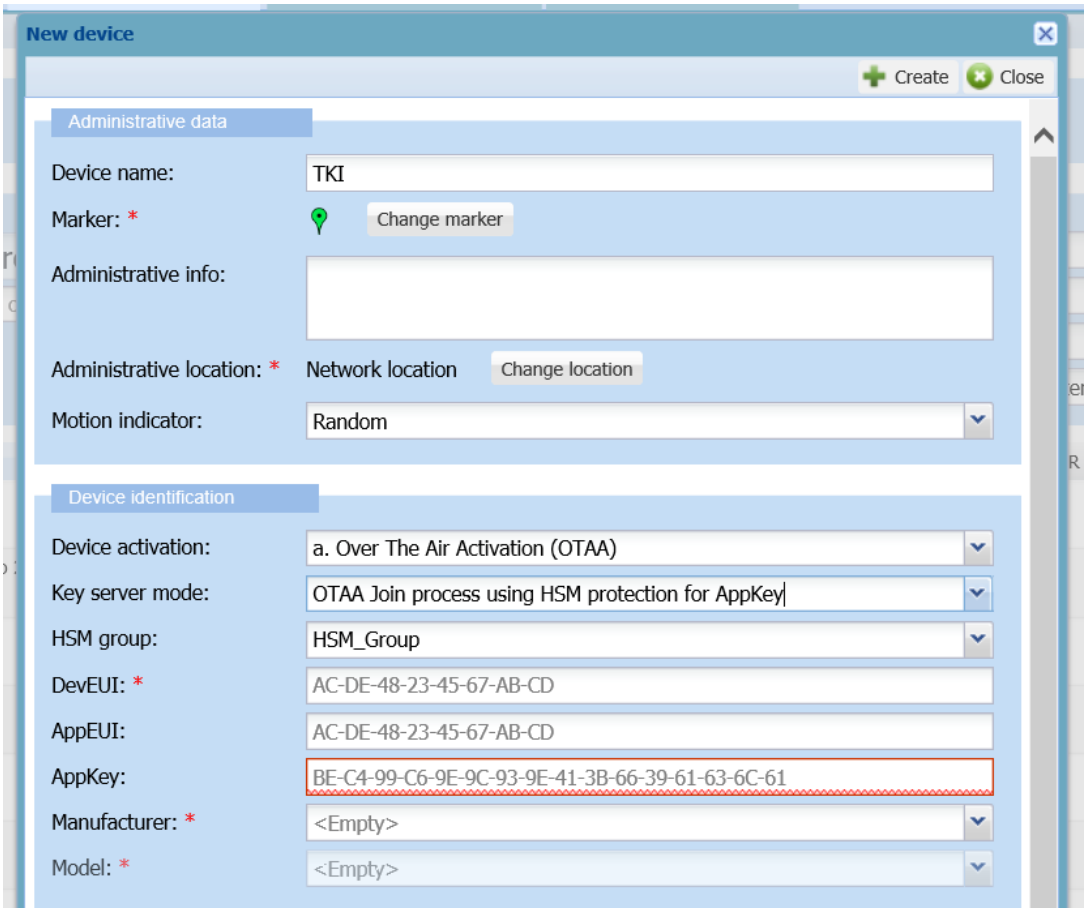
Recommendations done by Applied Risk:

1. Use OTAA instead of ABP.
2. Enable packet counter security to prevent replay attacks.
3. Make sure session keys are renewed before the packet counter overflows.
4. Use a different AppKey for every device or accept the risk that compromising one device allows manipulation and decryption of data traffic.
5. Implement anomaly detection to detect attacks like ACK spoofing, by monitoring sudden changes in packet counters or other properties.
6. Use TLS to encrypt communications between backend servers.
7. Perform security assessments on the eventual end devices and software to prevent implementation-specific exploitation via the LoraWan payloads.
8. Never use predictable encryption keys.

1: Use OTAA instead of ABP.

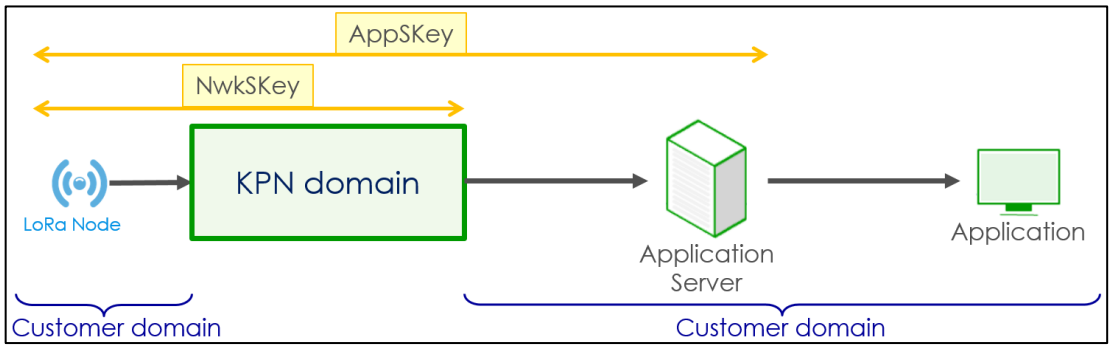
KPN only supports OTAA capable device to connect to their network. To connect a new OTAA device to the KPN LoRaWan network the customer can use the device manager or an API.

To prevent leaking of and for safely storing the keys, KPN uses a geographic redundant hardware security module (HSM) independent of the LoRaWan network server. A HSM is a physical computing device that safeguards and manages digital keys for strong authentication and provides crypto processing instead of storing the keys in a network server. The HSM also play a role in the E2E encryption of the sensor data which enables only the Application server to decrypt the payload of the sensor device.



Figuur 67: Device Manager

The LoRaWan protocol offers two layers of security implemented using the AES128 algorithm. On the network layer, the integrity of a message is enforced by the Message Integrity Code (MIC) and the payload is encrypted on the application layer. This means that it is possible to have end-to-end encryption of LoRa data. For LoraWAN the network keys used are in the KPN domain and the application keys are in the customer domain. They must comply to usage policies to prevent variables that are easy to guess. In the case of Over-The-Air Activation (OTAA) the used NwkSKey and AppSKey are managed from the KPN domain (Join service) and can be refreshed periodically. Figuur 68 shows the domain of the NwkSKey and the AppSKey.

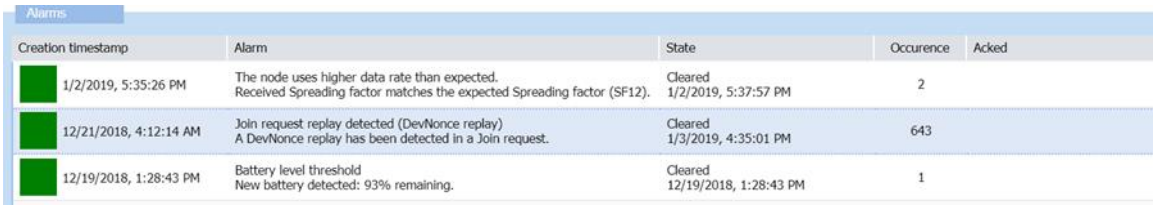


Figuur 68: NwkSKey and AppSKey domain

2 : Enable packet counter security to prevent replay attacks.

A Replay Attack Prevention mechanism is active in the network. This mechanism uses the frame counter (FCntUp) to determine whether an incoming message is valid. If a new message with the same counter as the previous message is sent, this message is ignored. This functionality applies to OTAA-devices. As a result of this mechanism, it is not possible to turn devices off after every message without storing the counter-value. Since switching the device off resets the counter value, the device will only send messages with FCntUp=1. This means that all messages will be ignored by the network and as a consequence the device will no longer pass messages to the Application Server.

The Alarms page in Thingpark (see below) will show warnings indicating a frame replay is blocked.



Figuur 69: Alarm display

The alarms can also automatically be sent to a Security Operation Center (SOC) of the customer. Independent of the detection of Replay attacks there are more alarms available which can indicate tampering with a device, for example unexpected battery levels.

Another way to ensure that the application data is checked, is to use Data Recovery through Application Layer Coding (DaRe[46]). DaRe is a data recovery method designed for LoRaWan. It allows to recover data from previously lost frames. DaRe is developed by Paul Marcelis and has been published in the 2nd ACM/IEEE International Conference on Internet of Things Design and Implementation (IoTDI 2017). In normal LoRaWan frames the payload contains the data to be received. This means when frames are dropped, the data from that frame is lost. Using DaRe

[46] See DaRe: Data Recovery through Application Layer Coding for LoraWan by Paul Marcelis, Vijay S. Rao, and R. Venkatesha Prasad, available at http://www.es.ewi.tudelft.nl/papers/2017-Marcelis-DaRe.pdf

Coding the data is processed before it is put in the payload of a frame. The data is extended with redundant information constructed from previous payloads. This redundant information can be used to reconstruct lost previous frames. If your application is using DaRe Coding, just tick the "Coding" box in the device settings, and the frames will be interpreted correctly.

Code: https://github.com/maerduq/dare-coding

3: Make sure session keys are renewed before the packet counter overflows.

When OTAA is used, the DevEUI, AppEUI and AppKey are needed to register the device on the network. The NwkSKey and AppSKey are derived from the AppKey when joining the network. The advice for the frequency of periodically rejoining depends on the number of messages sent by the End device and the level of security required to start a new Packet counter cycle.

A device should re-join:
- Every time it has lost the session context information
- Every x days
- Every y messages

The x and y values may differ depending on the level of security required; appropriate values could be once a month or maybe once every 2-3 months. The security risk depends on the application: metering applications sending a low amount of values typically do not need very frequent re-keying, while critical applications (e.g. alarms) would require more frequent re-keying. Currently KPN has no precise defined time or number of messages when a rejoin will be forced. Customers should make sure their device and application can still work and build a connection when a rejoin is required. During the OTAA Join, the network forwards the join message to the Application Server identified by the AppEUI. This Application Server is supposed to have been provisioned with the End device's AppKey.

Note. In LoRaWan 1.1 an additional Mac command will be introduced. With this new Mac command , Rejoin, it is also possible to request a rejoin from the network server. KPN has planned to introduce LoRaWan 1.1 in 2020.

4: Use a different AppKey for every device.

From the LoRaWan specification: "The 128-bit AppKey must be personalized in each device during production. It may be distinct per device or unique per application depending on the use-case. Providing the AppKey is the responsibility of the customer, such that the AppKey can be provisioned to the Application Server associated with the End device".

One of the conditions of the KPN LoRaWan service is that the device needs to be LoRaWan certified. During this certification process not only the uniqueness of the keys will be checked but also the correct entropy (composition of the keys). To help

with this process KPN provides tools to calculate AES 128 keys. By using OTAA the AppKey is replaced during the Join process by the AppSkey. A new AppSkey is calculated every time during the Join process.

5: Implement anomaly detection to detect attacks like ACK spoofing, by monitoring sudden changes in packet counters or other properties.

As described in (2) KPN also provides meta-data which contain the Frame Counter together with to data to the application server of the customer. This meta-data enables the Application server to detect certain anomalies, not only based on the packet counter but for example also unexpected location movements or changes in radio conditions. Example meta-data from KPN Network server and Customer Application server:

DevEUI_uplink message in the customer Application Server

```
>> POST <as-url>
?LrnDevEui=000000000F1D8693&LrnFPort=2&LrnInfos=UPHTTP_LAB_LORA&AS_I
D=app1.sample.com&Time=2016-01-
11T14%3A11%3A11.333%2B02%3A00&Token=fd0b0b00464aa798a59282d64eaa7081
3e33bff87682880db49638569d096aad
<?xml version="1.0" encoding="UTF-8"?> <DevEUI_uplink
xmlns="http://uri.actility.com/lora"> <Time>2015-07-
09T16:06:38.49+02:00</Time> <DevEUI>000000000F1D8693</DevEUI>
<FPort>2</FPort> <FCntUp>7011</FCntUp> <ADRbit>1</ADRbit> <ACKbit>1</ACKbit>
<MType>4</MType>
<FCntDn>11</FCntDn> <payload_hex>0027bd00</payload_hex>
<mic_hex>38e7a3b9</mic_hex> <Lrcid>00000065</Lrcid> <LrrRSSI>-
60.000000</LrrRSSI> <LrrSNR>9.750000</LrrSNR> <SpFact>7</SpFact>
<SubBand>G1</SubBand> <Channel>LC2</Channel> <DevLrrCnt>2</DevLrrCnt>
<Lrrid>08040059</Lrrid> <Late>0</Late>
<LrrLAT>48.874931</LrrLAT> <LrrLON>2.333673</LrrLON> <Lrrs> <Lrr>
<Lrrid>08040059</Lrrid> <LrrRSSI>-60.000000</LrrRSSI> <LrrSNR>9.750000</LrrSNR>
<LrrESP>-59.000000</LrrESP> </Lrr> <Lrr> <Lrrid>33d13a41</Lrrid> <LrrRSSI>-
73.000000</LrrRSSI> <LrrSNR>9.750000</LrrSNR> <LrrESP>-72.000000</LrrESP> </Lrr>
</Lrrs> <CustomerID>100000507</CustomerID> <CustomerData>...</CustomerData>
<ModelCfg>0</ModelCfg> <InstantPER>0.02</InstantPER> <MeanPER>0.02</MeanPER>
<DevAddr>0405F519</DevAddr>
<UplinkDC>0.001</UplinkDC>
<UplinkDCSubBand>0.009</UplinkDCSubBand>
<DevLocTime>2015-01-27T10:00:43.336+01:00</DevLocTime>
<DevLAT>10.11212</DevLAT>
<DevLON>7.44464</DevLON>
<DevAlt>50</DevAlt>
<DevLocRadius>100</DevLocRadius>
<DevAltRadius>50</DevAltRadius>
<DevNorthVelocity>1.0</DevNorthVelocity>
<DevEastVelocity>1.0</DevEastVelocity>
<NwGeolocAlgo>0</NwGeolocAlgo>
<NwGeolocTdoaOpt> 0</NwGeolocTdoaOpt>
</DevEUI_uplink>
```

6: Use TLS to encrypt communication between backend servers.

The connection between the KPN LoRa network and the customer Application Server uses Internet connectivity and the application connection is established using HTTPS. By using HTTPS, the confidentiality of the interface is managed and certificates ensure the identity of both the client and the server side. This setup not only encrypts the sensor data but also the meta-data which is exchanged between the network server and application server.

The connection between the KPN Network Server and the customer Application Server uses two separate authentications (one for the Application Server and one for the Network Server), which together lead to mutual authentication:

1. The customer Application Server needs to have a valid SSL certificate.
2. An authentication token is used within the application data stream to validate authenticity of the data.

These two levels of security are used in both uplink and in downlink messaging. Uplink messages are forwarded by the KPN LoRa server to the customer Application Server by using an HTTPS POST request. Within the connection setup, the identity of the customer Application Server is validated by checking the SSL certificate. The responsibility of retrieving the SSL certificate and keeping track of the validity lies with the customer. The KPN LoRa server accepts SSL certificates from most major SSL certificate authorities. When there is no certificate or if it is not valid, KPN will not forward the data. Tooling to test the validity of your SSL certificate can be found online, for example at https://www.ssllabs.com/ssltest/.

The authentication token mentioned as the second layer of security is calculated using SHA-256. The token is used to verify if the messages are sent from a valid source. The HTTPS POST request should contain a correctly calculated token. The recipient can confirm this token by recalculating the token with some information from the request and the shared secret LRC AS-Key. The LRC AS-Key is a configuration of the Application Server in ThingPark. Choosing a proper LRC AS-Key (and storing it safely on the customer Application Server) is the responsibility of the customer. There is an online tool available for generating an LRC AS-Key (for testing purposes) that has a sufficient Shannon entropy, at https://www.loratools.nl/#/keys. For the token verification, reference code is available on https://github.com/kpn-iot/lora-reference.

KPN not only encrypts the data between the network server and the application server but also other connections within its network. For example the connection between the gateway and the Network server independent of the type of connections used. And also the connection between the two redundant Network servers which are distributed over two locations.

7: Perform security assessments on the eventual end devices and software to prevent implementation-specific exploitation via the LoRaWan payloads.

To help customers with implementing security in their solutions, KPN publishes the KPN Security Policy online and created an App containing the KPN Security Policy (KSP). The KSP contains different aspects like physical security, business continuity and privacy. The KSP can be found on: https://github.com/KPN-CISO/kpn-security-policy

To keep up to date on security issues concerning LoRaWan the Lora-alliance published white papers on this topic. The white papers can be found on the website www.lora-alliance-org.