Rijkswaterstaat
Ministerie van Infrastructuur en Waterstaat

RWS INFORMATIE

AIS2025

Project Start Architectuur

Datum	7 februari 2023
Status	Definitief

Colofon

Uitgegeven door	Rijkswaterstaat Centrale Informatievoorziening
Informatie	Eric Blok
Telefoon	06-21890106
Uitgevoerd door	Pim Meij (CIV OSR SVMS)
Opmaak	CIV.PSA template 2.1
Datum	7 februari 2023
Status	Definitief
Versienummer	0.1

Versiebeheer

Versie	Status	Auteur	Opmerking
0.1	Concept	Pim Meij	Eerste versie die alleen de IST situatie beschrijft. Verzonden aan Kian Tan, Therry van der Burgt en Koen Lim.
0.2	Concept	Pim Meij	Aanpassingen naar aanleiding van overleg met Kian Tan. Gedeeld met AIS2025 team.
0.3	Concept	Pim Meij	Commentaar verwerkt van Eric Blok, Brian Langenberg en Koen Lim.
0.4	Concept	Pim Meij	Nagekomen commentaar op versie 0.1 verwerkt van Therry van der Burgt. Overzicht DISsen verwerkt van Corstiaan Mulckhuijse. Enterprise principes ingevuld naar aanleiding van eerste AIS2025 architectuursessie.
0.5	Concept	Pim Meij	Gegevensprincipes ingevuld naar aanleiding van tweede AIS2025 architectuursessie.
0.6	Concept	Pim Meij	Applicatieprincipes ingevuld naar aanleiding van derde AIS2025 architectuursessie.
0.7	Concept	Pim Meij	Technische principes ingevuld naar aanleiding van vierde AIS2025 architectuursessie.
0.8	Concept	Pim Meij	Beveiligingsprincipes ingevuld naar aanleiding van vijfde en

			laatste AIS2025 architectuursessie.
0.9	Concept ter review	Pim Meij	Hoofdstukken 1 en 2 ingevuld. Document gereed voor review.
0.10	Concept ter review	Pim Meij	Commentaar verwerkt van Eric Blok, Sander de Boer, Therry van der Burgt, Marcel Donker, Vincent Hol, Brain Langenberg, Koen Lim, Corstiaan Mulckhuijse, Wiemla Oppentocht, Frank Rakhorst en Harco Slot. Rondgestuurd voor controle op verwerking commentaar en nog enkele vragen uitgezet.
1.0	Definitief	Pim Meij	Beantwoorde vragen verwerkt en document Definitief gemaakt na akkoord CIV en VWM architecten en AIS2025 team.

Inhoud

1 Architectuur op hoofdlijnen voor AIS2025 7
1.1 Vraag 7
1.1.1 Klant 7
1.1.2 Klantbehoefte 7
1.2 Randvoorwaarden 8
1.2.1 Rijkswaterstaat InformatieVoorziening Aansluitvoorwaarden (RIVA) 8
1.2.2 Overige randvoorwaarden 9
1.3 Systeem context 9
1.4 Alternatieven en afwegingen 10
1.4.1 Alternatief 1 (gekozen alternatief) 10
1.4.2 Alternatief 2 11
1.4.3 Alternatief 3 11
1.4.4 Alternatief 4 11
1.5 Oplossingsarchitectuur 11
1.5.1 Informatievoorziening 11
1.5.2 Afwijking ten opzichte van de klantwens 12
1.5.3 Rationale gekozen oplossing 12
1.5.4 Afwijking ten opzichte van de RIVA 12
1.6 Open issues, risico's 13

2 Architectuur overzicht en walk & talk through 14
2.1 Architectuur overzicht 15
2.2 Walk & talk through 16

3 Bedrijfsarchitectuur 19
3.1 Requirements 19
3.2 Specifieke bedrijfskaders voor dit project 19
3.3 Dienstverleningsmodel, processen, organisatie en mensen 24
3.3.1 Impact 24
3.3.2 Bedrijfskoppelvlakken 26
3.3.3 Bedrijfsscope 28
3.3.4 Beheer 28

4 Informatie systeem architectuur (gegevens) 29
4.1 Specifieke informatie kaders voor dit project 29
4.2 Informatie en gegevensverzamelingen 33
4.3 Impact 37
4.3.1 Informatie scope 37
4.3.2 Informatie koppelvlakken 37
4.3.3 Beheer 37
4.3.4 Kwaliteitseisen 37

5 Informatie systeem architectuur (applicatie) 39
5.1 Specifieke applicatie kaders voor dit project 39
5.2 Applicatie componenten 43
5.2.1 Impact 43
5.2.2 Applicatie scope 48
5.2.3 Applicatie koppelvlakken 48
5.2.4 Beheer 50

5.2.5 Kwaliteitseisen 50

6 Technische Architectuur 51
6.1 Specifieke technische kaders voor dit project 51
6.2 Middleware, Platformen, Netwerkarchitectuur 53
6.2.1 Impact 53
6.2.2 Technische koppelvlakken 57
6.2.3 Technische scope 60
6.2.4 Beheer 62
6.2.5 Kwaliteitseisen 62

7 Beveiliging 63
7.1 Specifieke beveiligingskaders voor dit project 63
7.2 Beveiligingsmiddelen en maatregelen 65
7.2.1 Impact 65
7.2.2 Beveiliging scope 65
7.2.3 Beveiliging koppelvlakken 65
7.2.4 Beheer 65
7.2.5 Kwaliteitseisen 66

8 Industriële Automatisering 67

Bijlage Appendices 68
A.1 Referenties 68
A.2 Afkortingen en acroniemen 69

1 Architectuur op hoofdlijnen voor AIS2025

1.1 Vraag

1.1.1 Klant

RWS maakt sinds 2012 gebruik van een Automatic Identification System (AIS) oplossing van SAAB TransponderTech, in beheer bij SAAB Tein VOF (STV). Het contract voor het beheer en onderhoud van het core systeem en de base stations eindigt in 2025.

Een groot deel van de toegepaste IT componenten naderen het einde van zowel de technische als economische levensduur. Daarnaast is er volgens het [PID AIS2025] de wens om de huidige dienstverlening van AIS (vanaf 2025) te continueren en onderzoek te doen naar verbetermogelijkheden.

RWS CIV is daarom het project Vooronderzoek AIS2025 gestart. Deze Project Start Architectuur (PSA) is opgesteld ten behoeve van het project en daarmee indirect ook voor de afnemers van de dienstverlening van AIS.

Met deze PSA krijgen we goed inzicht in het huidige AIS (de *IST* situatie) en vervolgens doen we de uitwerking van het gewenste toekomstige AIS (de *SOLL* situatie).

1.1.2 Klantbehoefte

Volgens [PvA AIS Next] wordt het vooronderzoek in het tweede kwartaal van 2022 gestart en in het tweede kwartaal van 2023 afgerond. In het vooronderzoek komen tien onderwerpen aan de orde waarvan de volgende relevant zijn voor deze PSA:

“(1) Inzicht krijgen in het huidige AIS systeemconcept in lagen en bijbehorende functies, door
• Het in beeld brengen van de presentatie-, distributie-, verwerkings-, ontvang- en zendlaag
• Hoe monitoring en control is ingericht
• Een analyse van de betrokken componenten die bij de realisatie van de functies betrokken zijn. Deze analyse zal duidelijk maken welke componenten eventueel (door redundantie, overbodigheid) kunnen vervallen of onder een ander contract kunnen worden ingevuld

...

(3) Inzicht en overzicht krijgen in het huidige systeem landschap, door
• Modelleren van de huidige datastromen van- en naar de afnemende en aanleverende systemen zodat deze ook in het toekomstige systeem kunnen blijven werken.
• Gaandeweg nieuwe systemen in het landschap op te nemen of oudere te verwijderen. Door het contextdiagram periodiek bij te werken houden we zicht op het geheel

...

(4) Verkennen van de volgende scenario's voor de toekomstige situatie, door

...

• Uitwerken van scenario 2: optimalisatie huidig systeemconcept (modulaire opzet, daarbij alle functies beoordeelden en deze binnen/buiten scope brengen van nieuwe contract)

...

(9) Inzicht krijgen in de internationale AIS-standaarden, door
• Wijzigingen in kaart brengen sinds de vorige implementatie uit 2012 en deze vertalen naar eisen per object voor de toekomstige situatie
• Inventarisatie van te verwachten toekomstige wijzigingen (zoals VDES)

(10) De huidige- en toekomstige architectuur te schetsen, door
• Een PSA op te stellen waarin zowel de huidige- als de nieuwe architectuur wordt uitgewerkt
• Verschillende architectuuroverwegingen weloverwogen worden gemaakt en worden toegelicht
• Besluitvorming over de toekomstige architectuur kan plaatsvinden"

In de bovenstaande tekst is bij onderwerp (4) het door de Stuurgroep gekozen scenario 2 getoond. Dit scenario behelst het geheel of in delen naar de markt brengen van AIS dienstverlening, zie [Scenariokeuze]. Het doen van een uitspraak welke bestaande modules (componenten genoemd in dit document) we behouden en welke we opnieuw aanbesteden is een belangrijk doel van deze PSA. Het vormt daarmee een nadere uitwerking van dit scenario en maakt het concreet.

1.2 Randvoorwaarden

1.2.1 Rijkswaterstaat InformatieVoorziening Aansluitvoorwaarden (RIVA)

1. De oplossing kan volledig ingevuld worden met RIVA bouwstenen.
2. Voor de oplossing benodigde RIVA bouwstenen zijn beschikbaar maar voldoen functioneel niet. De benodigde wijzing op RIVA bouwstenen is beschreven in 1.5.
3. Voor de oplossing benodigde RIVA bouwstenen ontbreken. Het door het project op te leveren nieuwe RIVA bouwsteen is beschreven in 1.5
4. Voor de oplossing benodigde RIVA bouwstenen zijn beschikbaar maar er is een belemmering om deze te gebruiken. De explain m.b.t. de afwijking op RIVA bouwstenen is beschreven in 1.4 en 1.5.

De omkaderde optie 1 is voor de toekomstige AIS keten van toepassing.
De RIVA moet worden gelezen als landingsplatform voor domeinspecifieke business logica en we maken volledig gebruik van componenten uit die RIVA. Het is niet geëist dat domeinspecifieke business logica als bestaande RIVA bouwstenen beschikbaar is of tot nieuwe RIVA bouwstenen leidt.

1.2.2 Overige randvoorwaarden

De i-Strategie 2.0 is van toepassing. Met name de volgende onderdelen daaruit zijn leidraad voor de architectuurkeuzes in deze PSA:

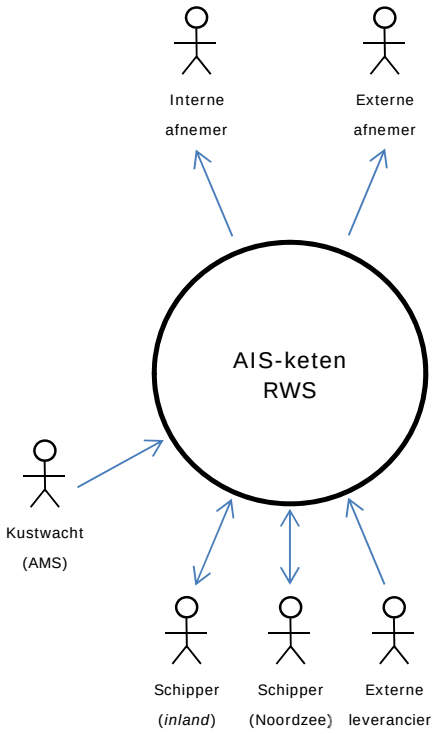
- “Rijkswaterstaat als samenwerkingsvaardige organisatie”, dit komt in dit document tot uiting in het gebruik van (RIVA) bouwstenen en een modulaire architectuur waarmee schaalbaarheid en daarmee schaalvoordeel zijn te bereiken;
- “Rijkswaterstaat moet meer uniformeren”, dit komt in dit document tot uiting in de standaardisering bijvoorbeeld met het National Marine Electronic Association (NMEA) protocol waarbij we aansluiten op internationale standaarden.
- Eis “Veiligheid door monitoring: objecten worden aangesloten op SOC en MKO”. In de praktijk zien we dat dit nog weinig gebeurt echter deze PSA schrijft voor dat er gebruik moet worden gemaakt van Splunk SIEM aan de kant van het Security Operations Center (SOC) en een syslog server op het AIS core systeem platform.

1.3 Systeem context

In de AIS keten onderscheiden we nu de volgende actoren en functionaliteiten:

- Inwinning van AIS berichten van schippers via de *inland* base stations van RWS;
- Inwinning van AIS berichten van schippers via de Noordzee base stations van RWS (Wind op Zee Wind Turbine Generator of Offshore Sub Station, NOGEPA olie- of gasplatform, onshore locatie, Europlatform);
- Inwinning van AIS berichten van schippers via AIS systemen van derden;
- Heruitzending van AIS berichten ontvangen van een regio in een andere regio ten behoeve van schippers die bij bochtige vaarwegen met obstructies anders niet met elkaar kunnen communiceren (wat AIS betreft);
- Verwerking van AIS berichten: decoderen, anonimiseren en aggregeren;
- Opslag van AIS berichten: short term storage en long term storage;
- Distributie van AIS berichten naar een veelheid aan interne RWS en externe afnemers ten behoeve van bijvoorbeeld visualisatie, fusie met radar en gegevensanalyse;
- Informeren van schippers met behulp van AMS (AIS Messaging Service); berichten, deze functie wordt nu alleen gebruikt door de Kustwacht.

Het standaard formaat is NMEA alhoewel wij zelf met de ADL ook in JSON formaat leveren (zie hoofdstuk 2 voor meer uitleg over de ADL).



Opmerking: Het is natuurlijk niet de schipper zelf die AIS berichten stuurt en ontvangt maar een *transponder*. Zo'n transponder kan ook op een reddingsvest zijn aangebracht of een SAR (Search and Rescue) transponder zijn, enzovoort. Voor het begrip hanteren we in dit document de meer aansprekende term schipper.

1.4 Alternatieven en afwegingen

Opmerking: Voor het begrip van de hieronder genoemde applicatiecomponenten is het raadzaam eerst hoofdstuk 2 te lezen. Het PSA template schrijft echter voor dat de alternatieven in dit hoofdstuk genoemd worden.

1.4.1 Alternatief 1 (gekozen alternatief)

Gegeven scenario 2: optimalisatie huidig systeemconcept, kiezen we voor het vervangen van de DIAMONIS core waaronder we verstaan CoastWatch, de AMS applicatie en het ERA systeem. Tevens worden de DISsen uitgefaseerd en hun functionaliteit wordt overgenomen door de ADL.

Voor de core functionaliteit zijn naast het CoastWatch systeem de AMS en ERA applicatie componenten ontwikkeld door SAAB. De hierin besloten functionaliteit maakt nu onderdeel uit van hun nieuwe Maritime Control COTS product. Ook andere leveranciers bieden deze functionaliteit.

De grotere rol voor de ADL is gebaseerd op de investeringen die RWS hierin heeft gedaan en de architectuurprincipes "Data is los van de applicatie beschikbaar" en "Hergebruik vóór kopen vóór maken" (zie hoofdstuk 5.1).

AIS2025 is een vervangingsproject maar het zorgt ook voor een nieuw beheer en onderhoud contract. En AIS2025 is een migratieproject aangezien de leveranciers en afnemers (voor een overzicht zie hoofdstuk 3.3.2) met een nieuw systeem zullen moeten gaan communiceren (het nieuwe core systeem voor leveranciers en de ADL voor afnemers).

1.4.2 Alternatief 2

Een andere mogelijkheid die is onderzocht, is behalve het vervangen van CoastWatch, AMS en ERA, ook de ADL te vervangen, alles door één nieuw core systeem.
De ADL is echter relatief recent ontwikkeld door RWS en biedt vele technische mogelijkheden voor het aansluiten van een in principe onbeperkt aantal afnemers vanwege de schaalbaarheid van deze applicatie. De ADL is daarmee de invulling van het architectuurprincipe “Data is los van de applicatie beschikbaar”.
Vervangen van de ADL zou voorts een desinvestering zijn en in strijd met het architectuurprincipe “Hergebruik vóór kopen vóór maken”.

1.4.3 Alternatief 3

Wellicht komt het nieuw aan te besteden core systeem met een complete GUI voor het visualiseren van het scheepvaartverkeer. Alhoewel we gebruik zullen maken van de GUI voor het beheer van het nieuwe core systeem en de base stations en het verzenden van AMS berichten, is het in eerste instantie niet de intentie om die GUI te gebruiken als vervanging voor de bestaande SVV. De SVV is een applicatie die weliswaar voor verbetering vatbaar is (en daar loopt op moment van schrijven ook een Basis Op Orde traject voor) maar de applicatie is stabiel genoeg om te behouden.

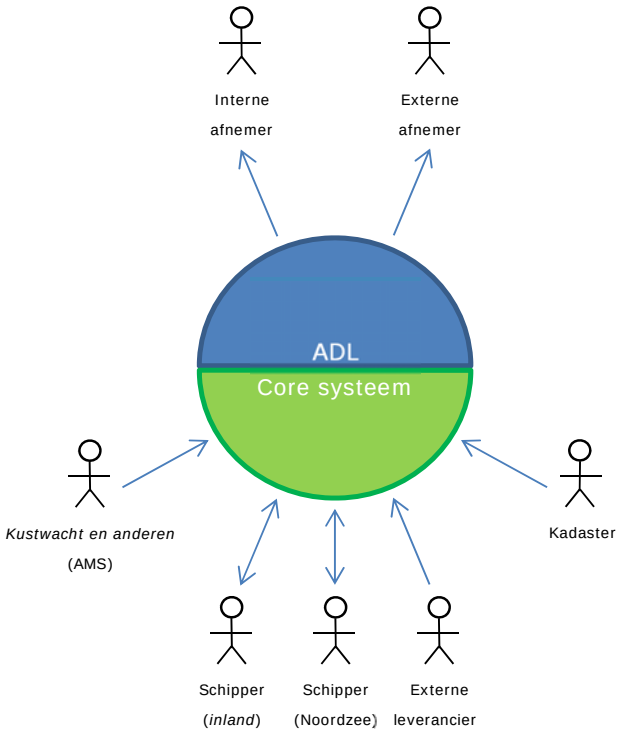
1.4.4 Alternatief 4

Het is nog overwogen om externe leveranciers direct te laten aansluiten op de ADL in plaats van op het nieuwe core systeem. Echter, het core systeem voert verschillende functies uit die niet in de ADL zitten zoals het ontdubbelen van AIS berichten en het beoogde verzamelen van metadata. Een voorbeeld van metadata is welk base station een AIS bericht heeft ontvangen. De Kustwacht heeft aangegeven behoefte te hebben aan deze informatie. Deze metadata zou via de GUI van het core systeem of een automatische koppeling dan relatief makkelijk kunnen worden ontsloten.
Verder willen we de ADL, de AIS *Distributie* Laag ook beperken tot distributie en deze niet uit laten groeien tot een monoliet zoals we die vroeger in ons applicatielandschap veel (en soms nog wel) tegenkomen.

1.5 Oplossingsarchitectuur

1.5.1 Informatievoorziening

De nieuwe AIS keten bestaat grofweg uit twee grote blokken: het nieuwe core systeem en de ADL.



Het nieuwe core systeem zorgt voor de uitwisseling van AIS berichten met de base stations van RWS. Ook externe leveranciers zijn op het core systeem aangesloten. Tevens verzorgt het nieuwe core systeem de AMS functionaliteit, voor de Kustwacht en mogelijk ook voor toekomstige (RWS) gebruikers werkzaam in het *inland* verkeersmanagement.
Het nieuwe core systeem krijgt een koppeling met het Kadaster voor het ontvangen van plaatsbepalingscorrecties die via de base stations aan schippers kunnen worden verzonden.

Voor AIS berichten wordt de NMEA standaard gebruikt maar het nieuwe core systeem is ook voorbereid op de VDES communicatiestandaard.

1.5.2 Afwijking ten opzichte van de klantwens

Er zijn geen afwijkingen ten opzichte van de klantwens zoals vastgelegd in [US AIS2025]. Met de blik op de toekomst hebben we ook alvast innovaties opgenomen waarvoor vermoedelijk een klantwens bestaat: corrigeren van GNSS locaties en het gebruik van VDES.

1.5.3 Rationale gekozen oplossing

De oplossing is gekozen op basis van het gekozen scenario 2 en de architectuurprincipes “Data is los van de applicatie beschikbaar” en “Hergebruik vóór kopen vóór maken”.

1.5.4 Afwijking ten opzichte van de RIVA

Er zijn geen afwijkingen ten opzichte van de RIVA, zie hoofdstuk 6.2.3.

1.6 Open issues, risico's

Er zijn voor de architectuur geen open issues of risico's geïdentificeerd.

2 Architectuur overzicht en walk & talk through

De voorliggende versie van de PSA beschrijft de huidige en gewenste toekomstige architectuur van AIS.

Deze architectuur wordt beschreven door een aantal modellen.

Een model is een simplificatie van de werkelijkheid. We modelleren zodat we het systeem dat we beschrijven of ontwikkelen beter kunnen begrijpen.
Omdat een model een simplificatie is, is één model, ofwel *view*, niet voldoende. Daarom beschrijven we het systeem met meerdere modellen, vanuit verschillende gezichtspunten, of wel *viewpoints*.

De volgende vier viewpoints worden toegepast:

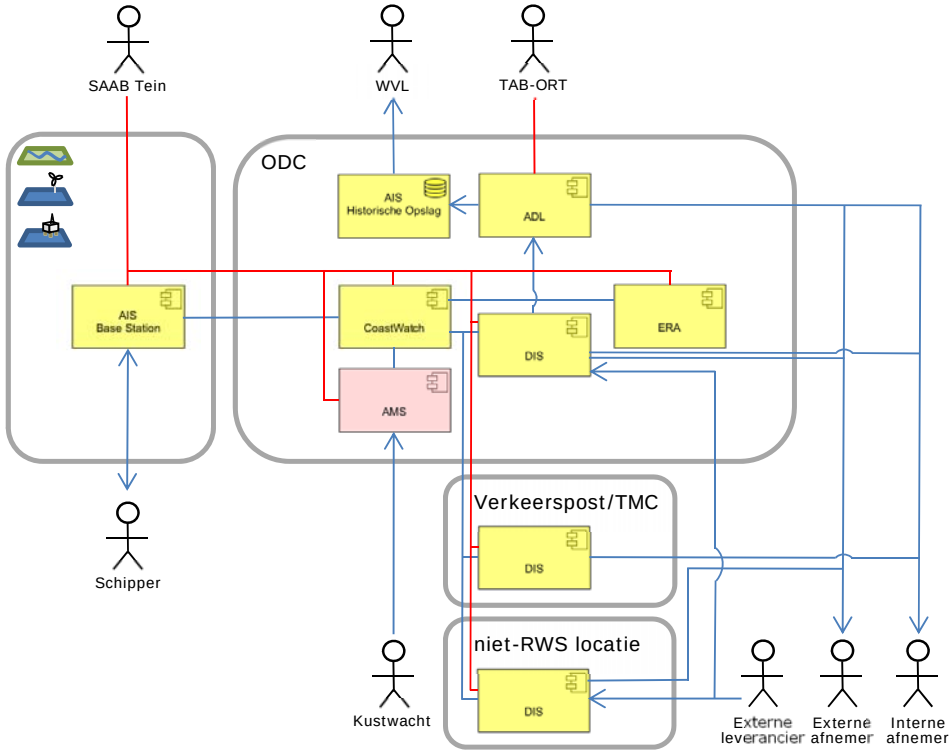
- *use case* view;
- *information design* view;
- *component interaction* view;
- *deployment* view.

De use case view beschrijft hoe het systeem zich gedraagt vanuit het perspectief van de gebruikers.
De information design view laat zien uit welke informatie artefacten het systeem bestaat.
De component interaction view laat zien uit welke software artefacten ofwel componenten het systeem bestaat, van welke informatie artefacten ze eigenaar zijn en hoe ze interacteren. We onderscheiden applicatie componenten en middleware componenten. Een component interaction view is een uitwerking van een use case of meerdere use cases.
De deployment view laat zien waar de componenten fysiek gehuisvest zijn.

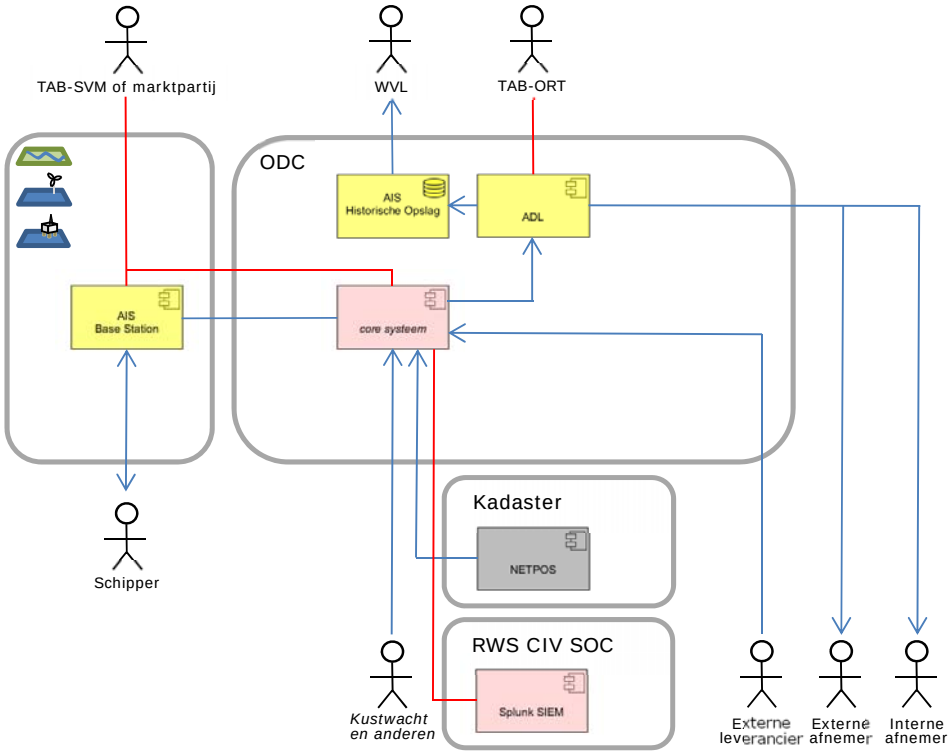
We maken gebruik van de Unified Modeling Language (UML). Dit is een standaard voor het visualiseren, specificeren, construeren en documenteren van de artefacten in een IV systeem. Zie [UML].

In dit hoofdstuk proberen we een totaal overzicht van de AIS-keten te krijgen, *IST* en *SOLL*. Het is daarbij onmogelijk om alle details van de vier viewpoints weer te geven in één overzicht. Daarom zijn alleen de belangrijkste kenmerken van de AIS-keten getekend en (met tekst) toegelicht. In de hoofdstukken hierna worden wel de vier viewpoints met alle details getekend en toegelicht.

2.1 Architectuur overzicht



Figuur 1: AIS-keten, IST situatie



Figuur 2: AIS-keten, SOLL situatie

2.2 Walk & talk through

De blauwe lijnstukken geven de functionele stroom van (AIS) data aan.
De rode lijnstukken geven het beheer aan.

Gele applicaties zijn RWS eigendom.
Roze applicaties zijn RWS eigendom met een user interface.
Grijze applicaties zijn externe dus niet-RWS applicaties.

IST:

Een AIS base station kan zich bevinden op een locatie *inland* of op de Noordzee. Voorbeeld van een *inland* locatie is de Papendrechtsebrug. Voorbeeld van een Noordzee locatie is Wind Turbine Generator B07 in het windmolenpark Borssele alpha. Ook kan een AIS base station zich op een NOGEPA olie- of gasplatform bevinden.

Ingewonnen AIS berichten van de scheepvaart in het NMEA formaat wordt tezamen met metadata vanaf het base station via switches en routers gerouteerd naar de CoastWatch applicatie welke geleverd is door SAAB en zich bevindt in het OverheidsDataCenter (ODC). CoastWatch distribueert de AIS berichten niet rechtstreeks maar altijd via een DIAMONIS Interface Server (DIS) naar de afnemers. Er zijn zowel RWS als externe dus niet-RWS afnemers.

Voor de interne afnemers staat een DIS meestal op de locatie waar de AIS berichten worden afgenomen, bijvoorbeeld op een Verkeerspost of op een sluis of brug. Daar worden de AIS berichten getoond in een lokale applicatie zoals bijvoorbeeld gefuseerd met radar data. Voor de interne afnemer LUV-VTS wordt echter van een DIS in het ODC gebruik gemaakt.
Voor de externe afnemers staat een DIS soms op hun eigen locatie en soms in het ODC.
Sommige externe afnemers zijn tegelijkertijd ook leverancier van AIS berichten (van de base stations waarvan zij eigenaar zijn). Een voorbeeld is de Schelde Radar Keten.
Ook de levering van AIS berichten gaat altijd via een DIS soms op hun eigen locatie en soms in het ODC.

Alle DISsen zijn eigendom van RWS of ze nu in het ODC staan, op een RWS locatie of op locatie bij een externe partij.

Een bijzondere afnemer van AIS berichten is de AIS Distributie Laag (ADL). De ADL is door RWS in het leven geroepen om niet teveel DISsen te hoeven kopen maar om de data zelf te distribueren naar een groot aantal afnemers. Dit kunnen weer interne en externe afnemers zijn. Daarnaast biedt de ADL de mogelijkheid de data in andere formaten dan NMEA te leveren bijvoorbeeld JSON. Ook kan de ADL anonieme data leveren in zowel NMEA als JSON formaat.

Een afnemer van de ADL is ook de AIS Historische Opslag. Deze heeft een short en een long term storage voor het opslaan van en leveren van de AIS berichten aan partijen zoals WVL voor verkeerskundige analyses. De opgeslagen AIS berichten kunnen, onder voorwaarden, ook gebruikt worden voor juridische doeleinden.

Opmerking: Op moment van schrijven is de AIS Historische Opslag nog niet in gebruik en dus ook niet in beheer. Echter dit wordt wel verwacht binnen afzienbare tijd.

Op CoastWatch heeft SAAB in opdracht van RWS nog twee modules gebouwd:

De AIS Messaging Service (AMS) is het systeem waarmee een gebruiker berichten voor de scheepvaart kan broadcasten in een bepaald gebied of berichten aan een specifieke (groep) schipper(s) sturen. Hiervoor heeft AMS een gebruikersinterface en aan de andere kant een koppeling met CoastWatch.
De Kustwacht is nu de enige gebruiker van AMS.

Met de External Repeater Application (ERA) worden AIS berichten van base stations binnen een geconfigureerde regio heruitgezonden naar andere regio's. Deze functionaliteit wordt gebruikt voor het Julianakanaal, waar vanwege de bochtige vaarweg schippers grote moeite hebben AIS berichten naar elkaar te sturen maar met ERA wordt dit alsnog mogelijk. Om overbelasting van het systeem te voorkomen is het ook mogelijk om slechts 1 op n berichten te heruitzenden.

CoastWatch, AMS en ERA vormen samen de DIAMONIS core waarbij DIAMONIS staat voor Dutch Inland AIS Monitoring System.

SAAB Tein doet het beheer van de base stations en van de DIAMONIS core en eveneens van alle DISsen.
Het ORT team beheert de ADL.

SOLL:

De scope van AIS2025 is het vervangen van de DIAMONIS core door één nieuw COTS product en het inregelen van beheer wat zowel intern als extern kan worden belegd.
Tevens wordt de rol van de DISsen als leverancier van AIS berichten overgenomen door de ADL.

In de toekomstige situatie zijn nog steeds de bestaande en ongetwijfeld nieuwe base stations *inland* en op de Noordzee. Deze communiceren straks met het nieuw aanbestede core systeem.

De levering van de AIS berichten, zowel aan interne als externe afnemers gaat nu via de ADL. Het core systeem zelf heeft daarmee nog maar één directe afnemer, zijnde de ADL.

Het nieuwe core systeem moet niet alleen geschikt zijn voor NMEA maar moet ook voorbereid zijn op VDES als nieuwe communicatiestandaard.

De levering van AIS berichten door externe leveranciers gaat direct op het core systeem. De ADL wordt dus wel gebruikt voor het leveren van AIS berichten maar niet voor het ontvangen hiervan (behalve natuurlijk die van het core systeem).

Het core systeem biedt een gebruikersinterface en een API voor het versturen van AMS berichten naar de scheepvaart en deze interface wordt wederom gebruikt door de Kustwacht en mogelijk anderen, bijvoorbeeld RWS zelf als besloten wordt dat RWS ook berichten naar de scheepvaart gaat sturen.

Het core systeem bevat ook de onder IST genoemde ERA functionaliteit.

Het core systeem krijgt verder een koppeling met het NETPOS systeem van het Kadaster voor het ontvangen en vervolgens doorsturen van AIS berichten aan de scheepvaart waarmee deze de plaatsbepaling via satelliet nauwkeuriger kan doen.

Tenslotte zal het core systeem zogenaamde events sturen naar het beveiligingssysteem Splunk waarmee het RWS CIV Security Operations Center (SOC) op basis van voorgedefinieerde regels een potentieel beveiligingsincident kan detecteren en hierop acteren.

Het technisch beheer van het core systeem en van de base stations gebeurt door een marktpartij, niet noodzakelijkerwijs de leverancier van het core systeem, en/of door TAB-SVM. Deze beslissing is nog niet genomen.
De ORT blijft verantwoordelijk voor het beheer van de ADL.

3 Bedrijfsarchitectuur

3.1 Requirements

Het document User stories AIS2025, [US AIS2025], beschrijft het concept van het toekomstige AIS informatiesysteem en de eisen aan het systeem in termen van werkprocessen.

De primaire functies van het AIS informatiesysteem zijn:

- Voor de decentrale infrastructuur (base stations, VHF antennes, GPS/GNSS antennes, bekabeling, beveiligingen tegen overspanning en voor aarding):
  - Het ontvangen van AIS berichten;
  - Het zenden van AIS berichten;
  - Het ontvangen, verwerken en zenden van berichten op basis van VDES;
- Voor de centrale infrastructuur (serverpark in het OverheidsDataCenter):
  - Het kunnen configureren en monitoren van de decentrale infrastructuur;
  - Het kunnen configureren en monitoren van de centrale infrastructuur;
  - Het ontvangen van en zenden naar de decentrale infrastructuur van AIS berichten;
  - Het zenden naar en ontvangen van interface toepassingen van AIS berichten;
  - Het ontdubbelen van AIS berichten;
  - Het heruitzenden (repeaten) van AIS berichten;
  - Het bewaren van metadata zodat een afnemer kan opvragen door welk base station een bericht is ontvangen, wat het tijdstip is waarop het bericht is ontvangen en wat de kwaliteit van het ontvangen bericht is;
  - Het bewaren van metadata zodat de applicatiemanager kan opvragen wat de kwaliteit van een ontvangen bericht is;
- Voor de interface toepassingen:
  - Het bieden van een GUI ten behoeve van het versturen van AMS berichten;
  - Het bieden van een API ten behoeve van het versturen van AMS berichten;
  - Het bieden van een GUI ten behoeve van het opvragen van metadata;
  - Het bieden van een GUI ten behoeve van triggers en filters;
  - Het bieden van historische opslag;
  - Het bieden van een geografische AIS viewer;
  - Het bieden van een distributielaag.

De systeemeisen zullen nader gespecificeerd worden in een System/Subsystem Specification (SSS).

3.2 Specifieke bedrijfskaders voor dit project

RWS werkt onder architectuur. Leidend zijn de architectuurprincipes (kaders). In dit hoofdstuk bekijken we de bedrijfskaders en hoe zij van invloed zijn op de nieuwe AIS keten.
De omkaderde enterprise kaders zijn van toepassing:

[EP-1] We werken als één landelijk opererende organisatie

[EP-2] We voeren de kerntaken uit met eigen mensen

[EP-3] We stemmen bij de uitvoering van onze taken af met onze stakeholders

[EP-4] Taken, verantwoordelijkheden en bevoegdheden zijn duidelijk, eenduidig vastgelegd en bekend

[EP-5] De “Regio” focust op de netwerkgebruikers en op de bestuurlijke partners, de “Landelijke uitvoering” focust op efficiëntie en standaardisatie

[EP-6] Samenwerken met anderen moet leiden tot verbetering van ons functioneren

[EP-7] Verandering moet bijdragen aan effectiviteit en efficiëntie

[EP-8] Beveiliging is integraal opgenomen in het ontwerp van processen

[EP-9] (principe is vervallen)

[EP-10] Eerst “hergebruik”, dan “kopen”, dan “laten maken”

	**EP-1: We werken als één landelijk opererende organisatie**
Dit houdt in:	Rijkswaterstaat ontwikkelt zich naar één geïntegreerd werkende organisatie, met één gezicht naar buiten, die gezamenlijk de ambities en de veranderende verwachtingen van onze omgeving waarmaakt.
Consequenties:	De ambitie voor AIS2025 is dat RWS dé data broker van Nederlandse AIS data is. Het nieuwe systeem moet één AIS infrastructuur bieden voor heel Nederland. Bijvoorbeeld de huidige situatie waarin West-Nederland Noord haar eigen AIS infrastructuur heeft en DIAMONIS niet gebruikt is niet efficiënt en niet gewenst. Het nieuwe systeem moet geschikt zijn voor het landelijk inwinnen van: - Inland data;

	- Noordzee data (de Kustwacht is eigenaar). Tevens moet het kunnen aansluiten op systemen van andere overheden ten behoeve van het inwinnen van: - Havenbedrijf Amsterdam data (gebeurt nu ook al); - Havenbedrijf Rotterdam data (gebeurt nu ook al); - Schelderadarketen data (gebeurt nu ook al).

Opmerking: Het is de vraag het project volgend op dit vooronderzoek AIS2025 ook het vervangen van het lokale systeem van West-Nederland Noord en het aansluiten van hun base stations op het nieuwe core systeem behelst. Zo niet, dan moet er een architectuurexceptie aangevraagd worden. Dit besluit is aan de Stuurgroep.

	**EP-2: We voeren de kerntaken uit met eigen mensen**
Dit houdt in:	Rijkswaterstaat kiest: welke taken doen we zelf? Wat kan de markt doen? Welke taken vervallen? Onze kracht is de professionele uitvoering van de kerntaken en de kennis, ervaring en creativiteit van de RWS-ers.
Consequenties:	Aangezien AIS missiekritieke functionaliteit betreft, wordt het beheer waar de tijd en om actie nemen en de betrouwbaarheid kritiek is zoveel mogelijk zelf gedaan of we laten het doen door de markt onder directe aansturing. Dit komt neer op: -Technisch beheer uitgevoerd door of onder directe aansturing van CIV OSR SVM TAB-SVM; -Applicatiebeheer uitgevoerd door CIV OSR SVM; -Functioneel beheer uitgevoerd door VWM BCC IBP of CIV OSR SVM.

	**EP-3: We stemmen bij de uitvoering van onze taken af met onze stakeholders**
Dit houdt in:	De maatschappij verwacht dat Rijkswaterstaat ervoor zorgt dat de werkzaamheden in goede onderlinge afstemming plaatsvinden.
Consequenties:	Indien de dienstverlening verandert wordt dit doorgevoerd in de bestaande Service Level Agreements (SLA's) met VWM en JIVC (de beheer- en onderhoudspartij van de Kustwacht). GegevensLeveringsOvereenkomsten (GLO's) betreffende directe koppelingen met DISsen gaan veranderen als gevolg van het

	verdwijnen van de DIS als component (de dienstverlening blijft hetzelfde overigens).

	**EP-4: Taken, verantwoordelijkheden en bevoegdheden zijn duidelijk, eenduidig vastgelegd en bekend**
Dit houdt in:	Rijkswaterstaat werkt als één team samen. Ieder draagt vanuit zijn eigen rol bij aan het resultaat. Heldere en korte sturingslijnen, gestandaardiseerde werkprocessen en gebundelde taken helpen daarbij.
Consequenties:	De volgende afspraken worden aangepast als gevolg van de nieuwe dienstverlening: -Governance kaart; -Governance plaat; -Informatieformulier van MKO; -Escalatiemodel; -Service Level Agreement (SLA) inclusief procesplaten; -Dossier Afspraken en Procedures (DAP); -Dossier Financiële Afspraken (DFA) met leverancier en JIVC; -GegevensLeveringsOvereenkomst (GLO).

	**EP-5: De “Regio” focust op de netwerkgebruikers en op de bestuurlijke partners, de “Landelijke uitvoering” focust op efficiëntie en standaardisatie**
Dit houdt in:	Om als beste uit de strijd te komen, moeten organisaties een keuze maken uit drie waardedisciplines (Treacy en Wiersema): operational excellence, product leadership of customer intimacy. De keuze van RWS ligt vast in het principe.
Consequenties:	Aangezien AIS missiekritieke functionaliteit betreft, kiezen we voor **operational excellence**.

	**EP-6: Samenwerken met anderen moet leiden tot verbetering van ons functioneren**
Dit houdt in:	Door met anderen samen te werken, kunnen we ons functioneren zo verbeteren, dat we aan de eisen van de maatschappij kunnen blijven voldoen.
Consequenties:	Eisen worden opgesteld met alle stakeholders. Dit is reeds ten dele gebeurd (middels de user stories, [US AIS205]) en ten dele gaan we dat nog doen (voor de SSS).

	**EP-7: Verandering moet bijdragen aan effectiviteit en efficiëntie**
Dit houdt in:	Verandering is nodig om verdere verbeteringen aan te brengen en om Rijkswaterstaat robuust te maken voor de toekomst.
Consequenties:	We gaan niet een op een vervangen, we stellen alles ter discussie. Als we het AIS-systeem enkel vanuit de technische noodzaak vervangen, missen we de kans om aan te sluiten bij de behoefte van de enterprise. Dit betekent dat er dus ook aandacht moet zijn voor de aansluiting bij de trends in de operationele bedrijfsvoering van verkeersmanagement en crisismanagement en welke winst in efficiëntie en effectiviteit we nastreven op het gebied van bedrijfsbehoefte en informatiebehoefte. We kijken serieus maar tegelijkertijd kritisch naar de ontwikkelingen in internationale standaarden bijvoorbeeld VDES. We zorgen voor betere contracten dan de huidige: dat wil zeggen effectiever, met betere mogelijkheden voor het sturen op prestatie en kwaliteit en wat verder nog uit de contractanalyse komt. We vernieuwen infrastructuur waar deze End Of Life (EOL) is: zowel decentrale (oude base stations) als centrale infrastructuur (de DIAMONIS core). Apparatuur die nog niet EOL is blijven we duurzaam inzetten.

	**EP-8: Beveiliging is integraal opgenomen in het ontwerp van processen**
Dit houdt in:	Beveiliging is een lijnverantwoordelijkheid en vormt een onderdeel van de kwaliteitszorg voor bedrijfs- en bestuursprocessen en de ondersteunende informatiesystemen.
Consequenties:	Security by design is en wordt toegepast. Het Security Operations Center (SOC) is en wordt meegenomen in onze besluitvorming. We hanteren de Privacy by design aanpak. Over Nationale Veiligheid wordt nagedacht en we vullen het hiervoor beschikbare sjabloon in (dit is verplicht bij iedere inkoop door de CIV).

	**EP-10: Eerst “hergebruik”, dan “kopen”, dan “laten maken”**

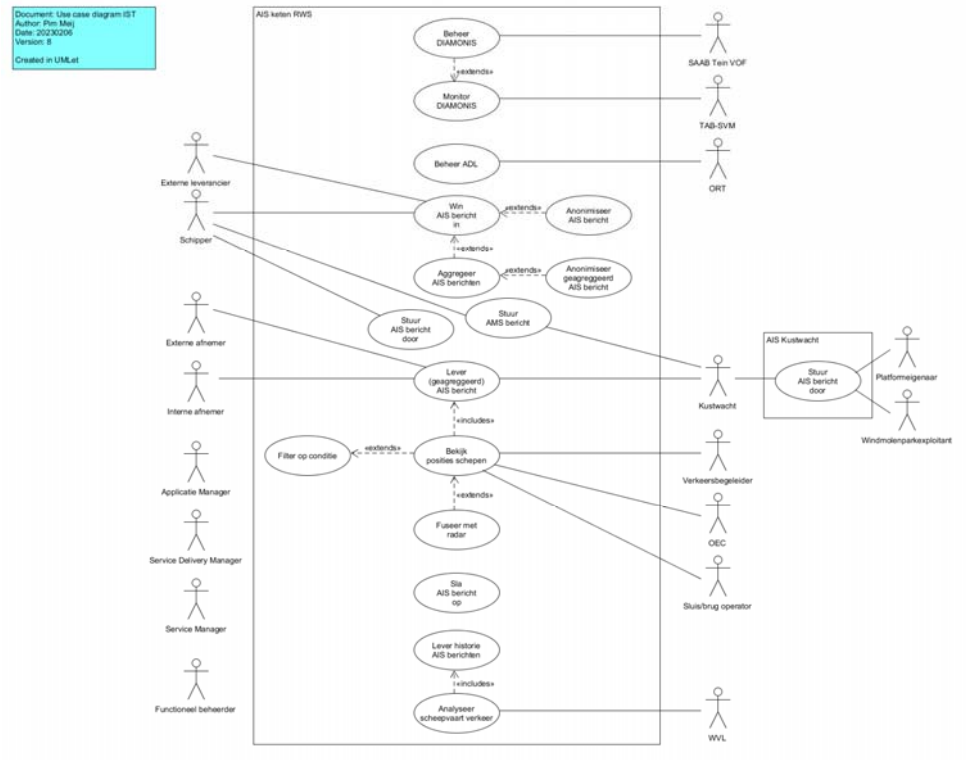
Dit houdt in:	Rijkswaterstaat is, als onderdeel van de overheid, eraan gehouden om duurzaamheid te bevorderen en kostenbewust te handelen. Hergebruik is goedkoper, omdat hiermee dubbele investeringen worden vermeden.
Consequenties:	De recent aangeschafte Saab R60 base stations houden we, voor base stations die op het eind van hun levensduur zijn gekomen en voor nieuwe inwinlocaties kopen we nieuwe bij. De functionaliteit van de DIAMONIS core en de bijbehorende DISsen besteden we opnieuw aan want deze zijn EOL. De ADL houden we en passen we aan wegens de reeds gedane investering en positionering. De AMS én de repeater functionaliteit vragen we uit bij de uitbesteding van een nieuw core systeem.

3.3 Dienstverleningsmodel, processen, organisatie en mensen

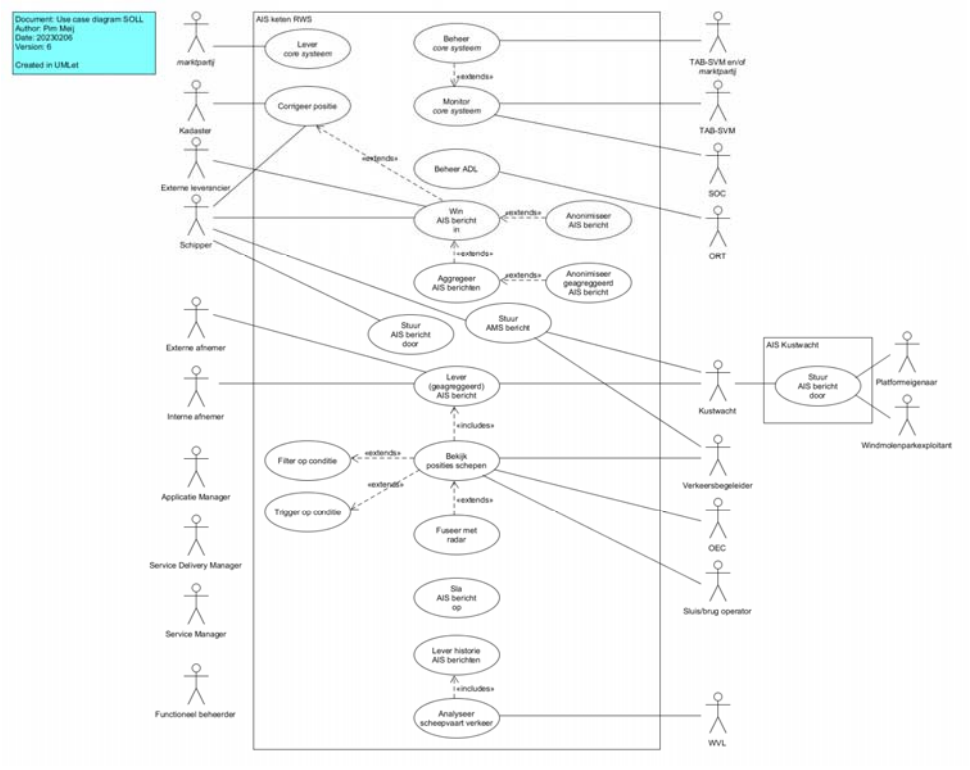
3.3.1 Impact

De gebruikers zijn het belangrijkste ‘onderdeel’ van het IV systeem. Het IV systeem is hier de “AIS keten RWS”.

De use case views van de AIS keten RWS, met de actoren en welke use cases voor hen relevant zijn, is gemodelleerd in de volgende UML *use case diagrams*:



Figuur 3: AIS IST, Use case view – Use case diagram



Figuur 4: AIS SOLL, Use case view – Use case diagram

Voor meer informatie over de use cases zie de user stories in [US AIS2025].

De verschillen tussen IST en SOLL zijn:

- Een mogelijk nieuwe marktpartij levert een AIS core systeem;
- DIAMONIS wordt vervangen door een nieuw core systeem, een COTS product, en dit wordt door wordt door TAB-SVM en/of een nieuwe marktpartij (hoeft niet dezelfde te zijn als de leverancier) beheerd en door TAB-SVM gemonitord;
- Het Kadaster levert GNSS correcties die via het core systeem aan een schipper geleverd worden waarmee deze de plaatsbepaling kan corrigeren;
- Een Verkeersbegeleider van RWS kan ook AMS berichten sturen;
- Er is een nieuwe use case ten behoeve van het triggeren op condities;
- Het SOC doet actieve monitoring van het nieuwe core systeem.

Het doel van AIS2025 is niet om de leveranciers en afnemers te wijzigen alhoewel in de loop de tijd er natuurlijk altijd leveranciers en afnemers bij kunnen komen. Voor een volledig overzicht van de huidige situatie zie hoofdstuk 3.3.2.

3.3.2 Bedrijfskoppelvlakken

- **Marktpartij**
  Levert het nieuwe core systeem en beheert dit eventueel.
- **Kadaster**
  Levert GNSS correcties waarmee een **Schipper** de plaatsbepaling kan corrigeren.

- **Externe leverancier**
  Een niet-RWS leverancier, niet zijnde een **Schipper**, van AIS informatie. We onderscheiden momenteel:
    - Kustwacht;
    - Havenbedrijf Amsterdam;
    - Havenbedrijf Rotterdam;
    - Schelderadarketen.
- **Schipper**
  Levert AIS informatie, ontvangt AIS informatie van naburige **Schipper** dankzij de repeater functionaliteit, ontvangt GNSS correcties afkomstig van het **Kadaster** en ontvangt AMS berichten van **Verkeersbegeleider**.
- **Externe afnemer**
  Een niet-RWS afnemer, niet zijnde een **Schipper** of de **Kustwacht**, van AIS informatie. We onderscheiden momenteel:
    - TenneT;
    - Provincie Noord-Holland;
    - Euris;
    - Vake;
    - Dirkzwager;
    - Havenbedrijf Amsterdam;
    - Havenbedrijf Rotterdam;
    - Schelderadarketen.
- **Interne afnemer**
  Een RWS afnemer van AIS informatie. We onderscheiden momenteel:
    - Verkeerspost Den Helder (RAF);
    - Verkeerspost Dordrecht (RAF);
    - Volkeraksluis (RAF);
    - Topshuis (RAF);
    - Verkeerspost Tiel (RAF);
    - Verkeerspost Nijmegen (RAF);
    - Verkeerspost Wijk bij Duurstede (RAF);
    - Krammersluis (RAF);
    - Kreekraksluis en –brug (RAF);
    - Vuurtoren Brandaris (?);
    - IVSNext;
    - SVV;
    - LUV VTS.
- **Applicatie Manager**
  Een functie bij CIV OSR SVM Services.
- **Service Delivery Manager**
  Een functie bij CIV OSR SVM Services.
- **Service Manager**
  Een functie bij CIV OSR SVM Services.
- **Functioneel beheerder**
  Een functie bij VWM BCC IBP.
- **TAB-SVM**
  Een team dat het nieuwe core systeem monitort en eventueel beheert.
- **ORT**
  Een team dat de ADL ontwikkelt en beheert.
- **Kustwacht**
  Een afnemer van AIS informatie en gebruiker van AMS.

- **Verkeersbegeleider**
  Een werknemer op een verkeerspost verantwoordelijk voor het begeleiden van de scheepvaart en in de toekomst wellicht gebruiker van AMS.
- **OEC**
  Rijkswaterstaat heeft de intentie als IV Serviceprovider op de Noordzee op te treden. Ook wil Rijkswaterstaat het onderzoek naar onder meer het mariene ecosysteem en de maritieme veiligheid op de Noordzee faciliteren. Hiervoor is het Offshore Expertise Centrum (OEC) opgericht.
- **Sluis/brug operator**
  Een werknemer op een sluis of brug of in een bediencentrale verantwoordelijk voor het bedienen van de sluis of brug.
- **WVL**
  Een afnemer en de eigenaar van historische AIS informatie ten behoeve van analyse
- **SOC**
  Het Security Operations Center SOC monitort op security incidenten.

De aanduiding (RAF) betekent dat de afnemer de AIS data gecombineerd met radardata bekijkt: Radar AIS Fusion. De aanduiding (?) betekent dat ik niet weet hoe de AIS data wordt bekeken.

3.3.3 Bedrijfsscope

De bedrijfsscope is de AIS keten vanaf het base station via het nieuwe core systeem en de ADL als distributeur en de koppelvlakken met de gebruikers en leverende en afnemende systemen.

3.3.4 Beheer

Het functioneel beheer is belegd bij VWM IV Beheer en Projecten, deze afdeling is ook de systeem eigenaar van de AIS keten.

4 Informatie systeem architectuur (gegevens)

4.1 Specifieke informatie kaders voor dit project

RWS werkt onder architectuur. Leidend zijn de architectuurprincipes (kaders). In dit hoofdstuk bekijken we de informatiekaders en hoe zij van invloed zijn op de nieuwe AIS keten.
De omkaderde informatiekaders zijn van toepassing:

[GP-1] Gegevens voldoen aan de wet

[GP-2] Gegevens volgens standaarden

[GP-3] Gegevens onder governance

[GP-4] Gegevens zijn geclassificeerd

[GP-5] Gegevens zijn toegankelijk

[GP-6] Gegevens voor organisatiedoelen

[GP-7] Gegevens hergebruik vóór inwinnen

[GP-8] Gegevens zijn toekomstvast

[GP-9] Gegevensstructuur is geborgd (dit principe is tegenwoordig opgenomen in [GP-12])

[GP-10] Gegevenskwaliteit is geborgd

[GP-11] Gegevens zijn koppelbaar (dit principe is tegenwoordig opgenomen in [GP-12])

[GP-12] Gegevens zijn voorzien van metadata

Opmerking: [GP-5] is niet van toepassing omdat AIS gegevens géén open data is vanwege de privacy. [GP-12] heeft geen gevolgen omdat AIS gegevens aan internationale standaarden (zoals NMEA) voldoen en, metadata of niet, een gegeven zijn binnen AIS2025.

	**GP-1: Gegevens voldoen aan de wet**

Dit houdt in:	RWS dient bij het inwinnen, verwerken, vastleggen, analyseren, ontsluiten en vernietigen van gegevens altijd te voldoen aan wet- en regelgeving. Basisregistraties en Open data zijn wettelijke verplichtingen die domein-overstijgend zijn en dus in elk project gecheckt moeten worden. Echter er zijn nog vele andere wettelijke verplichtingen die mogelijk onderdeel van de projectscope moeten zijn. Je moet dan denken aan: Europese Hergebruikrichtlijn 2003/98/EG, WION en INSPIRE. Ook is er Sectorspecifieke wet- en regelgeving zoals de Waterwet, KRW, Swung en de Europese ITS richtlijn. Bij de start van een project zal altijd met medewerkers van het desbetreffende domein moeten worden gecheckt welke overige wettelijke verplichtingen voor het project gelden. Deze activiteit zal vaak pas kunnen worden uitgevoerd bij de realisatie van de projectbrief of het PID **en is de verantwoordelijkheid van de projectleider**. Maar in de PSA moet wel worden vermeld dat dit onderdeel van de projectscope dient te zijn. Meer informatie over de, op dit moment, bekende wettelijke verplichtingen: http://corporate.intranet.rws.nl/Organisatie/Processen/Informatievoorziening/Inrichting_proces/Besturen_van_IV/Architectuur/Enterprisearchitectuur/RWS_Gegevensarchitectuur/RWS_Gegevensprincipes/ Kies in de rechterkolom voor document “Wettelijke en beleidsmatige kaders voor IV”.
Consequenties:	AIS informatie van RWS is géén open data en wordt niet vastgelegd in een basisregistratie voor ontsluiting naar de burger! Wel vindt gecontroleerde distributie van AIS-data plaats naar afnemers. RWS is gerechtigd om AIS informatie in te winnen, op te slaan en te distribueren. Al deze activiteiten maar met name de kwetsbare opslag dienen met voldoende beveiliging te gebeuren. Daartoe dient in de uitvoering van het project een privacy coördinator te worden ingeschakeld die *privacy by design* toepast.

	**GP-2: Gegevens volgens standaarden**
Dit houdt in:	RWS-gegevens worden volgens standaarden vastgelegd en uitgewisseld.
Consequenties:	We hanteren de internationale AIS standaarden, deze zijn vastgelegd in [Standaarden]. Voor de leveringen door de ADL is het bestaande document [IRS ADL] de zelf ontwikkelde en reeds gebruikte standaard op OSI

	laag 7 niveau (die overigens wel gebruik maakt van standaard technieken voor de lagere OSI lagen) en dit wordt hergebruikt.

	**GP-3: Gegevens onder governance**
Dit houdt in:	Rollen, taken, verantwoordelijkheden voor het totale gegevensleveringsproces heeft RWS eenduidig vastgelegd en toegewezen.
Consequenties:	De rollen, taken en verantwoordelijkheden zijn voor de hele AIS-keten vastgelegd in [US AIS2025] maar zullen nog per component moeten worden vastgelegd, bijvoorbeeld in een RACI-tabel.

	**GP-4: Gegevens zijn geclassificeerd**
Dit houdt in:	RWS classificeert gegevens volgens beveiligingsrichtlijnen. Deze classificatie bepaalt in welke mate beveiligingsmaatregelen noodzakelijk zijn.
Consequenties:	De AIS informatie is geclassificeerd in [PIA]. Deze is nog steeds geldig. Het nemen van beveiligingsmaatregelen wordt geborgd door het doen van een BIO-toets, deze is reeds gestart.

	**GP-6: Gegevens voor organisatiedoelen**
Dit houdt in:	Van gegevens(verzamelingen) is altijd duidelijk hoe deze bijdragen aan de missie en taken van RWS.
Consequenties:	Hoe de AIS informatie bijdraagt aan de missie en taken van RWS is vastgelegd in [US AIS2025].

	**GP-7: Gegevens hergebruik vóór inwinnen**
Dit houdt in:	RWS wint gegevens voor overeenkomstige informatiebehoeften eenmalig in, en gebruikt ze vervolgens meermalig.

	Basisregistraties Er zijn momenteel wettelijke basisregistraties voor de volgende data: topografie, ondergrond, kadastrale data, adressen, persoonsgegevens, kentekens, WOZ waarden, inkomens en bedrijfsgegevens uit het Handelsregister. Indien het project één van deze datasoorten gebruikt, dient deze data vanuit de Basisregistratie te worden betrokken. Voor topografie en ondergrond geldt daarnaast dat RWS ook bronhouder is, en dus data moet aanleveren. Een project moet dus rekening houden met het feit dat data ook na het project nog kan worden geleverd en nog steeds aan de wettelijke eisen voldoet. LET OP: formeel gelden de basisregistraties alleen bij de uitvoering van een publiekrechtelijke taak. Echter RWS gebruikt Basisregistraties ook voor niet publiekrechtelijke taken. Een voorbeeld: een aanlegproject gebruikt voor een Europese aanbesteding het Handelsregister. Een ander project voor de aankoop van kantoorartikelen houdt een eigen leveranciers bestand bij. Dit leidt ertoe dat RWS meerdere, bijna identieke, bestanden inkoopt en beheert. Deze situatie is onwenselijk en gaat in tegen de uitgangspunten van de i-Strategie RWS. Factsheet met meer informatie over (het gebruik van) basisregistraties: http://nwr-ipvw-sas005/PMWiki/Wiki.jsp?page=Bibliotheek%20met%20handige%20links (kies optie “Factsheets basisregistraties”)
Consequenties:	AIS informatie is géén open data en wordt niet vastgelegd in een openbare basisregistratie! Daar waar mogelijk gebruiken we AIS informatie die afkomstig is van infrastructuur van derden. We gebruiken de bestaande AIS Historische Opslag voor meerdere doelen zoals onderzoek bij incidenten, opsporing en het plannen van onderhoud aan de vaarwegen.

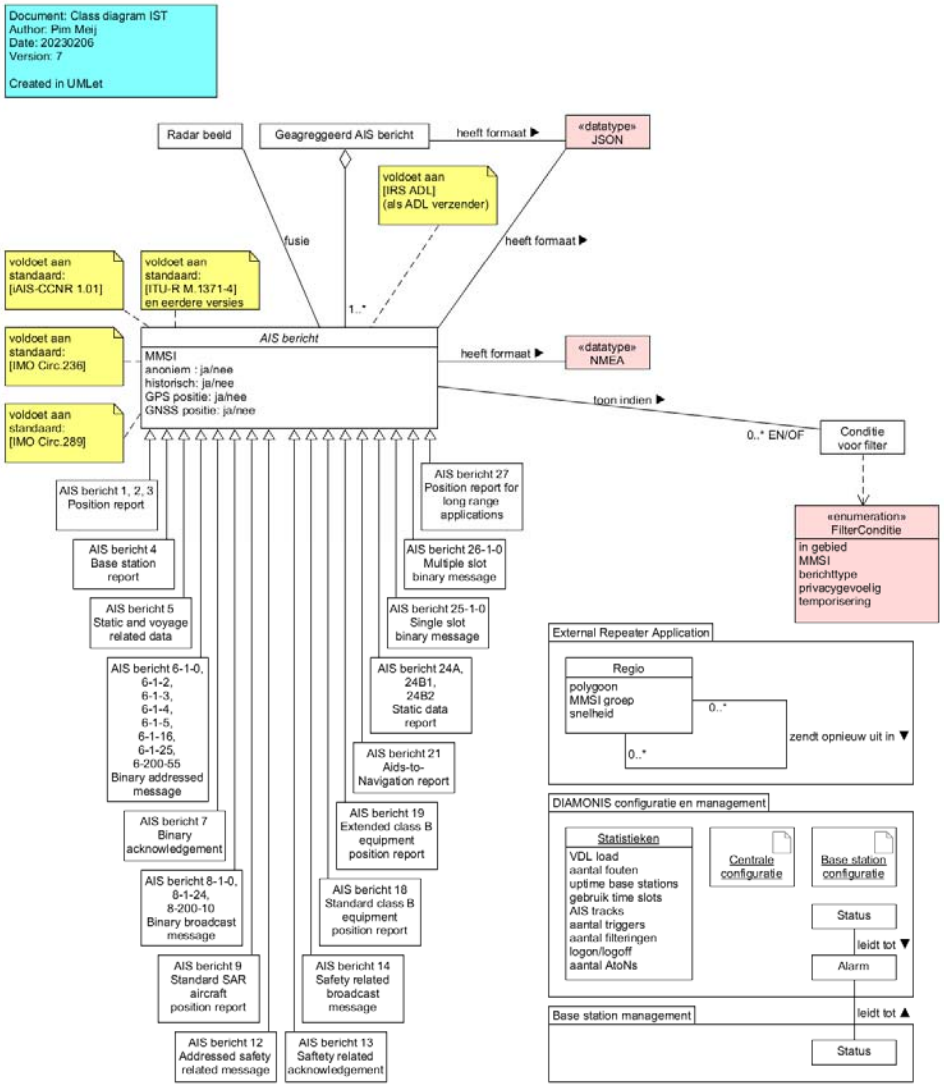
	**GP-8: Gegevens zijn toekomstvast**
Dit houdt in:	Gegevens zijn zolang als nodig beschikbaar en bruikbaar.
Consequenties:	Dit wordt bereikt met de bestaande AIS Historische Opslag.

	**GP-10: Gegevens kwaliteit is geborgd**
Dit houdt in:	De afgesproken kwaliteit van de gegevens is gegarandeerd. Algemeen bekend, in orde en de kwaliteit blijft in orde.
Consequenties:	Voor AIS2025 zijn 3 kwaliteitsaspecten erg belangrijk: - De informatie is *beschikbaar*, aangezien AIS als missiekritiek is bestempeld: dit betekent een *service window* van 24x7 en hersteltijd van < 4 uur; - De informatie is *tijdig*: voor sommige afnemers zoals RAF mag de periode tussen ontvangst van een bericht door het base station tot afleveren bij de afnemer die de fusie van AIS informatie met radardata doet maximaal 500 milliseconden zijn; - De informatie is *betrouwbaar*: plaatsbepaling dient gecorrigeerd te worden met DGNSS zodat de locatie maximaal 10 meter afwijkt. Spoofing dient gedetecteerd te worden en jamming dient voorkomen te worden. **Opmerking:** Spoofing (het met opzet versturen van foutieve AIS berichten) en jamming (het al dan niet met opzet verstoren van AIS signalen) zijn moeilijk te detecteren, en indien gedetecteerd zijn het volgens richtlijnen met betrekking tot deze onderwerpen veelal handmatige acties die genomen moeten worden. Automatische detecteren of voorkomen is daarom nu niet te garanderen. Deze eisen kunnen daarom het beste als optioneel bij de aanbesteding van een nieuw core systeem worden meegegeven: we gebruiken wat het core systeem of base station biedt.

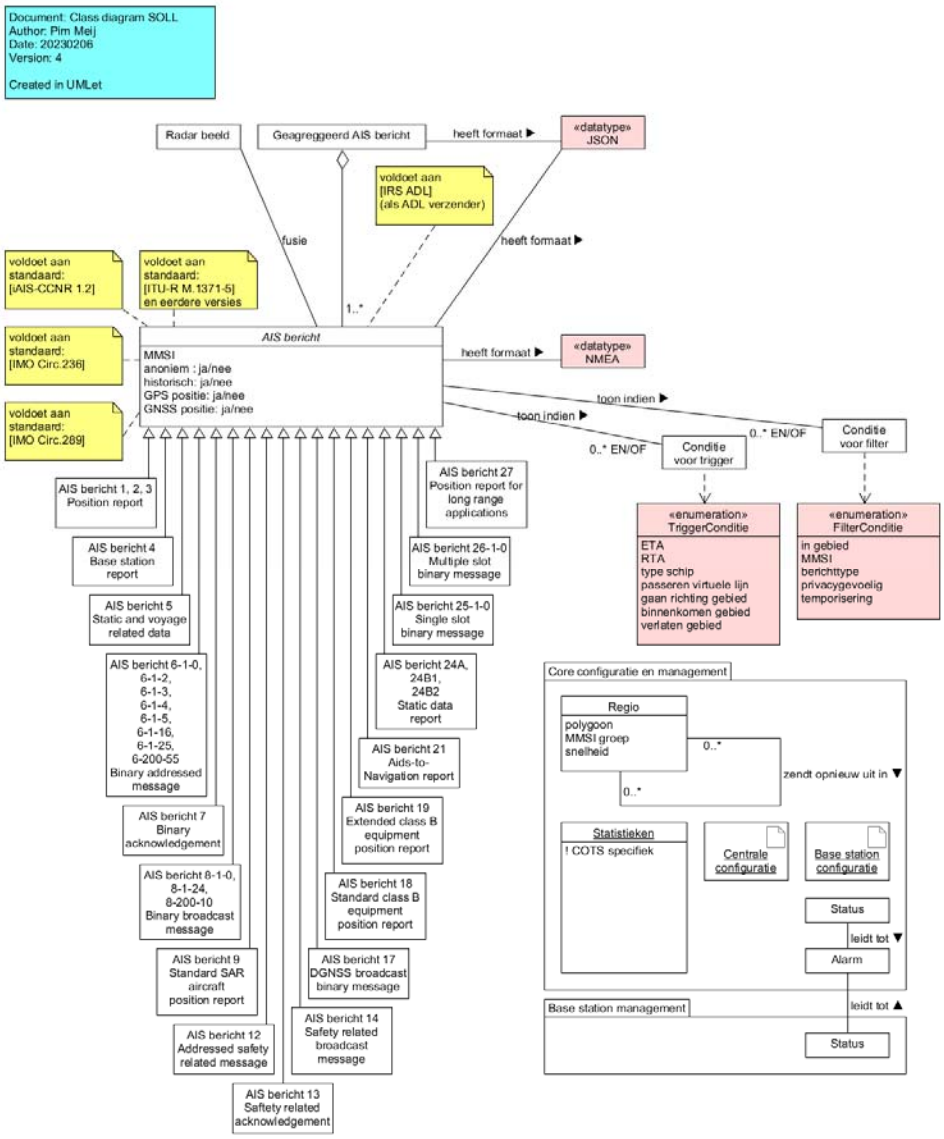
4.2 Informatie en gegevensverzamelingen

Na de gebruikers is informatie het belangrijkste onderdeel van een IV systeem. Het acroniem IV staat dan ook voor Informatievoorziening.

De information design view met de informatie artefacten die in de bestaande AIS keten bij RWS en haar partners een rol spelen, is gemodelleerd in de volgende UML *class diagrams* voor IST en SOLL:



Figuur 5: AIS IST, Information design view – Class diagram



Figuur 6: AIS SOLL, Information design view – Class diagram

De informatie artefacten zijn als volgt. Tevens wordt het verschil tussen de IST en de SOLL situatie gegeven.

AIS bericht De berichten die van schip naar gebruiker gaan en omgekeerd. De berichten voldoen in de IST situatie aan de internationale standaarden [ITU-R M.1371-4] en eerdere versies, [iAIS-CCNR 1.01], [IMO Circ.236] en [IMO Circ.289]. De berichten voldoen in de SOLL situatie aan de internationale standaarden [ITU-R M.1371-5] en eerdere versies, [iAIS-CCNR 1.2], [IMO Circ.236] en [IMO Circ.289]. Alle AIS berichten worden door DIAMONIS cq. het toekomstige core systeem en de ADL ontvangen en verzonden in ruw NMEA formaat maar alleen de expliciet getekende AIS berichten (1, 2, 3, enzovoort) worden door de ADL ook nog in geaggregeerd JSON formaat verzonden conform [IRS ADL].

Verder moet in de SOLL situatie ook AIS bericht 17 kunnen worden gegenereerd en verzonden. Het is een bericht met DGNSS-correcties dat door een base station aan de scheepvaart wordt verzonden waarmee een AIS transceiver aan boord van een schip de op basis van GNSS bepaalde locatie kan verbeteren (mits de transceiver hiervoor is uitgerust).
Een AIS bericht bevat het unieke MMSI nummer van een schip. Een AIS bericht kan echter ook geanonimiseerd zijn. In het geval van een positiebericht bevat het AIS bericht tevens de locatie van het schip bepaald met GPS of een ander GNSS systeem (bijvoorbeeld Galileo). Een AIS bericht kan ook naar de historische opslag worden geschreven.
Ieder AIS bericht zal mogelijk in de toekomst voldoen aan de VDES standaard.

Geaggregeerd AIS bericht Niet ieder AIS bericht dat een schip verzendt, bevat alle statische data, deze worden slechts eenmaal per 6 minuten verzonden. De meeste berichten bevatten slechts dynamische data. De ADL heeft de mogelijkheid te allen tijde een geaggregeerd AIS bericht te sturen waarin ook de statische data zijn meegenomen.

NMEA / JSON De berichten worden in NMEA of JSON formaat afgeleverd bij een afnemer. Een enkel bericht kan zowel in NMEA als in JSON formaat worden afgeleverd. Geaggregeerde berichten worden alleen in JSON formaat afgeleverd.

Radar beeld De AIS berichten en de radar worden gebruikt voor Radar AIS Fusion (RAF): het genereren van een nieuwe/verbeterde (geografische) positie van een specifiek contact. Dit gebeurt aan de hand van een wiskundige functie waarbij de informatie van de beide individuele contacten wordt gebruikt. Indien er geen sprake van een berekening is, spreken we van verrijken. Hierbij wordt de informatie van een contact verrijkt met de informatie van het andere contact. Dit is dan de informatie van hetzelfde contact maar vanuit een verschillende sensor. Bijvoorbeeld en afhankelijk van de gebruikte applicatie worden bij de bewegende punten op het radarscherm de naam van het schip, de vorm, de afmetingen en de vaarrichting van het schip weergegeven.

Regio Ten behoeve van de repeater functionaliteit kunnen regio's worden gedefinieerd waarvan de ontvangen AIS berichten worden heruitgezonden naar andere regio's. Een regio is gedefinieerd als een polygoon en eventueel kunnen alleen berichten binnen een bepaalde MMSI groep worden heruitgezonden. Ook wordt de snelheid ingesteld die aangeeft hoe vaak berichten afkomstig van één MMSI en met hetzelfde berichtnummer mogen worden heruitgezonden.
De regio's verhuizen van IST naar SOLL van de External Repeater Appliation naar de nieuwe core.

Centrale configuratie Er wordt in CoastWatch een centrale configuratie bijgehouden met instellingen voor het core systeem. Ook in het toekomstig core systeem zal dit moeten gebeuren.

Base station configuratie Met behulp van CoastWatch worden aangesloten base stations van SAAB geconfigureerd en opgeslagen. Met het toekomstige core systeem moeten base stations van verschillende fabrikanten vanuit het core systeem kunnen worden geconfigureerd en deze moeten uiteraard ook worden opgeslagen.

Status De status van CoastWatch en de base stations wordt nu bijgehouden. Ook het toekomstige core systeem zal zijn eigen status en die van de base stations moeten bijhouden.

Alarm Indien een status daartoe aanleiding geeft, wordt een beheerder van CoastWatch nu geïnformeerd middels een alarm. Ook in het toekomstige core systeem zal dit moeten gebeuren.

Conditie voor trigger Als een eindgebruiker geattendeerd dient te worden indien aan een conditie is voldaan, dan kan deze conditie of een combinatie van condities worden ingesteld. Dit was wel geëist voor de IST situatie en CoastWatch biedt deze functionaliteit maar hier wordt nu geen gebruik van gemaakt. Voor het toekomstige core systeem in de SOLL situatie stellen we deze eis niet maar voor de AIS keten wel (dit betekent dat bijvoorbeeld de SVV dit voor zijn rekening neemt). Een conditie kan zijn de verwachtte aankomsttijd (ETA), de gevraagde aankomsttijd (RTA), het type schip, het passeren van een virtuele lijn, het bewegen richting een gebied, het binnenkomen van een gebied, of het verlaten van een gebied.

Conditie voor filter Als een eindgebruiker alleen die schepen wil zien die aan een conditie voldoen, dan kan deze conditie of een combinatie van condities worden ingesteld. Dit was wel geëist voor de IST situatie en CoastWatch biedt deze functionaliteit maar hier wordt nu geen gebruik van gemaakt. Het wordt echter wel in de ADL toegepast: er kan gefilterd worden op gebied (*geofencing*), MMSI nummer, berichttype en privacy gevoelige data. Voorts kan er getemporiseerd worden. Voor het toekomstige core systeem in de SOLL situatie stellen we deze eis niet meer maar het blijft in de ADL.

Statistieken CoastWatch verzamelt allerlei statistieken zoals de VHF Data Link load, het aantal gedetecteerde fouten, de uptime van de base stations, het gebruik van time slots door de base stations, de AIS tracks (historie van 2 maanden), hoe vaak er getriggerd wordt op een conditie, hoe vaak er gefilterd wordt op een conditie, hoe vaak er wordt aangelogd op en uitgelogd van het systeem, en hoeveel AtoN berichten er worden verzonden van CoastWatch naar een schip. Ook in het toekomstig core systeem zullen statistieken worden verzameld om het goed te kunnen beheren, maar deze zullen specifiek voor dat systeem zijn.

4.3 Impact

4.3.1 Informatie scope
AIS berichten voldoen in de SOLL aan nieuwe standaarden.
Het gebruik van AIS bericht 17 is nieuw.
Triggers en de condities die hiervoor gemaakt kunnen worden zijn nieuw.

4.3.2 Informatie koppelvlakken
Er zijn geen (koppelvlakken) met omliggende gegevensverzamelingen.

4.3.3 Beheer
Het beheer van de historische AIS data is en blijft ondergebracht bij AIS applicatiemanagement, afdeling CIV OSR SVM Services.

4.3.4 Kwaliteitseisen

De real time informatie is beschikbaar: aangezien AIS als missiekritiek is bestempeld: dit betekent een service window van 24x7 en hersteltijd van < 4 uur;
De real time informatie is tijdig: voor sommige afnemers zoals RAF mag de periode tussen ontvangst van een bericht door het base station tot afleveren bij de afnemer maximaal 500 milliseconden zijn (ADL neemt hiervan zo blijkt uit metingen maximaal 200 milliseconden voor zijn rekening);
De real time en historische informatie is betrouwbaar: plaatsbepaling dient gecorrigeerd te worden met DGNSS zodat de locatie maximaal 10 meter afwijkt, optioneel dient spoofing gedetecteerd en jamming voorkomen te worden.

5 Informatie systeem architectuur (applicatie)

5.1 Specifieke applicatie kaders voor dit project

RWS werkt onder architectuur. Leidend zijn de architectuurprincipes (kaders). In dit hoofdstuk bekijken we de applicatiekaders en hoe zij van invloed zijn op de nieuwe AIS keten.
De omkaderde applicatiekaders zijn van toepassing:

[AP-1] Koppelen van industriële automatisering en administratieve automatisering alleen met voldoende beveiliging

[AP-2] Applicaties worden ontworpen voor optimale samenwerking met partners

[AP-3] RWS gebruikt standaarden

[AP-4] Gegevens worden eenmalig ingewonnen en beheerd, en meervoudig gebruikt (dit principe is tegenwoordig opgenomen in [GP-7])

[AP-5] Vernieuwing en groot onderhoud vinden plaats onder architectuur

[AP-6] Nieuwe applicaties bieden herbruikbare functionaliteit aan op basis van services (dit principe is tegenwoordig opgenomen in [AP-9])

[AP-7] Nieuwe applicaties die algemeen gebruikt worden, bieden een webbased user interface

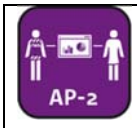
[AP-8] Data is los van de applicatie beschikbaar

[AP-9] Hergebruik vóór kopen vóór maken

[AP-10] Standaard pakketten gebruiken zoals geleverd

	**AP-1: Koppelen van industriële automatisering en administratieve automatisering alleen met voldoende beveiliging**
Dit houdt in:	Koppelen van industriële automatisering en kantoorautomatisering alleen met voldoende beveiliging.
Consequenties:	We passen authenticatie en gegevensencryptie toe tussen de verschillende applicatie componenten op basis van TLS. (SSL 2.0 en 3.0 mogen niet meer gebruikt worden).

	We gebruiken MAC filtering op de switch voor de base stations zodat alleen die base stations een connectie kunnen maken met het RWS netwerk. Binnen RWS maken we gebruik van een eigen AIS VPN. Derden zoals de Kustwacht verbinden we middels de RIVA bouwsteen IPsec koppeling via internet of de RIVA bouwsteen vaste externe toegangsvoorziening, bovendien maken we gebruik van een firewall.

	**AP-2: Applicaties worden ontworpen voor optimale samenwerking met partners**
Dit houdt in:	Applicaties worden ontworpen voor optimale samenwerking met partners.
Consequenties:	De samenwerking uit zich in het uitwisselen van AIS berichten met de partners. Deze is optimaal omdat gebruik gemaakt wordt van internationale standaarden waardoor internationale samenwerking tussen landen mogelijk is geworden door toepassing en uitwisseling van AIS data, zie bijvoorbeeld Euris.

	**AP-3: RWS gebruikt standaarden**
Dit houdt in:	RWS gebruikt standaarden, dit principe bevordert het gebruik van standaard producten en de uitwisseling van gegevens binnen en buiten Rijkswaterstaat.
Consequenties:	Uitgangspunt is ten eerste conform internationale standaarden (IALA, IMO, ITU en CCNR) producten en dienstverlening in te richten. Daaropvolgend wordt voldaan aan RWS standaarden.

	**AP-5: Vernieuwing en groot onderhoud vinden plaats onder architectuur**
Dit houdt in:	Zowel onderhoud als nieuwbouw van een applicatie kan de applicatiearchitectuur en daarmee de kosten van de applicatieportfolio maken of breken. Nieuwbouw en onderhoud van de applicatieportfolio gebeuren dus onder dezelfde applicatiearchitectuur.
Consequenties:	De applicatiearchitectuur van de AIS keten is in de afgelopen jaren uitgebreid en “vervuild” geraakt door onder andere dubbele

	functionaliteit in dezelfde portfolio. Uitgangspunt van deze PSA is om een bijgewerkte en schone portfolio te realiseren met één core systeem, de base stations, de ADL, en de AIS Historische Opslag.

	**AP-7: Nieuwe applicaties die algemeen gebruikt worden, bieden een webbased user interface**
Dit houdt in:	Applicaties voor algemeen gebruik, moeten breed kunnen worden verspreid. Webtechnologie biedt hiervoor goede mogelijkheden.
Consequenties:	Voor bestaande applicatie componenten die interactie met de gebruiker bieden worden reeds webbased user interaces gebruikt. Voorbeelden zijn SVV, AIS Historische Opslag en AMS. Voor het nieuw aan te besteden core systeem eisen we ook dat dit webbased is. (Daarmee zijn we ook onafhankelijk van het Operating Systeem).

	**AP-8: Data is los van de applicatie beschikbaar**
Dit houdt in:	Gegevens mogen niet worden opgesloten in een applicatie omdat gegevens vaak een langere levensduur én bredere toepasbaarheid kennen dan individuele applicaties.
Consequenties:	Met de ADL en de AIS Historische Opslag houden we bewust de distributie en business logica met betrekking tot verrijking/verarming alsmede de opslag buiten de scope van het nieuwe AIS core systeem. Hiermee zijn flexibiliteit en uitbreidbaarheid in de toekomst geborgd. Voor real time data is de ADL een reeds gebouwd systeem. Ten behoeve van het veiligstellen en later opvraagbaar maken van AIS gegevens is de AIS Historische Opslag een reeds gebouwd systeem. Deze systemen blijven in de nieuw architectuur bestaan en daarmee wordt aan dit applicatieprincipe voldaan.

	**AP-9: Hergebruik vóór kopen vóór maken**
Dit houdt in:	Nieuwe klantwensen vullen we eerst in met bestaande applicaties uit de applicatieportfolio of RIVA. Kan dit niet, dan kopen we een standaard applicatie. Pas als die niet op de ICT-markt verkrijgbaar is, start er een maatwerk-traject.

Consequenties:	Voor de real time levering van AIS gegevens aan interne en externe afnemers wordt op dit moment nog veel gebruik gemaakt van de DIS. Veelal wordt een DIS ingezet als 1 op 1 koppeling (alhoewel een DIS tot 4 afnemers aankan) en voor iedere DIS moet betaald worden zowel bij aanschaf als tijdens beheer, en dit maakt het een dure oplossing waarbij we bovendien slechts beperkt filtermogelijkheden hebben. Tenslotte hebben we met de grote hoeveelheid DISsen ook een navenant grote leveranciersafhankelijkheid. Daarom is door RWS de AIS Distributie Laag (ADL) ontwikkeld. De ADL biedt vele mogelijkheden voor het aansluiten van afnemers, uitgebreide filtermogelijkheden, en manieren van connectiviteit zoals JSON berichten maar ook tekststrings met de ruwe NMEA berichten over eenvoudige socketverbindingen. Voor de levering van historische AIS gegevens is door RWS heel recent speciaal de AIS Historische Opslag ontwikkeld. Deze is gebaseerd op het SAS platform en functioneert naar volle tevredenheid van de gebruikers. Voor de core functionaliteit zijn naast het CoastWatch systeem de AMS en ERA applicatie componenten ontwikkeld door SAAB en de hierin besloten functionaliteit maakt nu onderdeel uit van hun nieuwe Maritime Control COTS product. Ook andere leveranciers bieden deze functionaliteit. De SVV is een applicatie die weliswaar voor verbetering vatbaar is maar stabiel genoeg is om te behouden. Aangezien we gekozen hebben voor scenario 2 waarin we zelf niet gaan bouwen maar het huidige systeemconcept optimaliseren (modulaire opzet, daarbij alle functies beoordeelden en deze binnen/buiten scope brengen van nieuwe contract) kiezen we voor: - Hergebruiken van de ADL die we positioneren als dé distributie component voor AIS real time data; - Hergebruiken van de AIS Historische Opslag; - Behouden van de SVV; - Opnieuw aanbesteden van de core functionaliteit, die momenteel gerealiseerd wordt met de applicatie componenten CoastWatch, AMS en ERA.

	**AP-10: Standaard pakketten gebruiken zoals geleverd**
Dit houdt in:	Standaardpakketten worden geconfigureerd binnen de mogelijkheden van het standaardpakket. Zo kunnen we het standaardpakket, inclusief configuratie, makkelijk naar een volgende versie brengen.

Consequenties:	Conform [AP-3] gebruiken we standaarden en worden dit producteisen. De markt heeft op basis van deze standaarden reeds COTS producten ontwikkeld waardoor het gebruik van RWS van zo'n COTS product ook kan geschieden op basis van een standaard configuratie. (Feitelijk heeft RWS zelf bijgedragen aan de wording van de internationale standaarden en de applicatiebouwer heeft op basis daarvan de applicatie gebouwd). We zijn niet voornemens om zelf code aan de COTS applicatie toe te voegen omdat dit de mogelijkheid tot upgraden beperkt. We gebruiken de standaard functionaliteit en beperken ons tot het configureren van de applicatie.

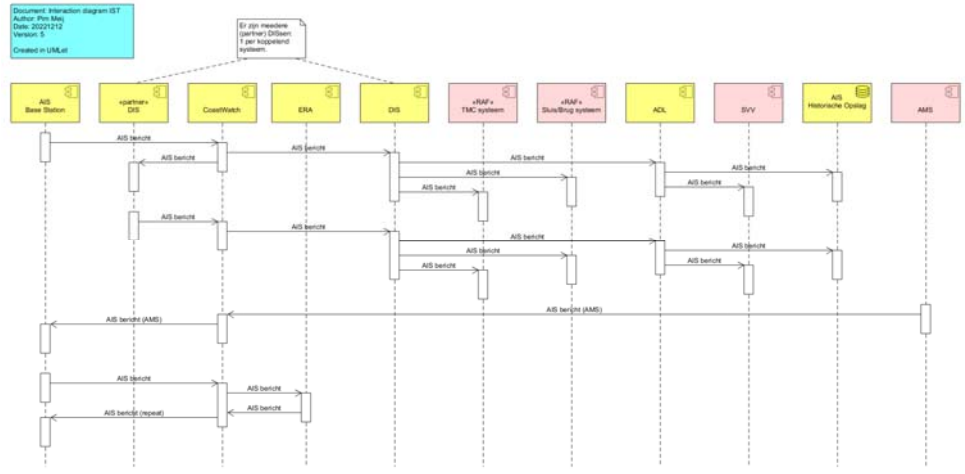
5.2 Applicatie componenten

5.2.1 Impact

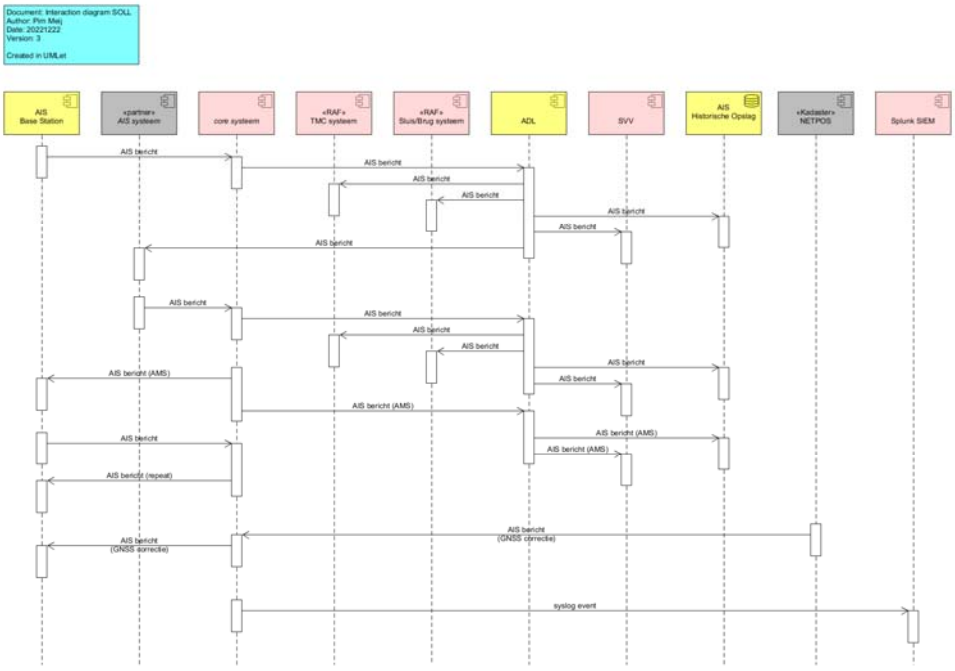
Het IV systeem voorziet de gebruikers van de juiste informatie dankzij de interacties tussen verschillende applicatie componenten.

Opmerking: Behalve de applicatie componenten zijn er ook middleware componenten, deze worden behandeld in hoofdstuk 6.2.1.

De component interaction view met de applicatie componenten en hoe zij interacteren in de bestaande AIS keten bij RWS en haar partners, is gemodelleerd in de volgende UML *interaction diagrams* voor IST en SOLL:



Figuur 7: AIS IST, Component interaction view – Interaction diagram



Figuur 8: AIS SOLL, Component interaction view – Interaction diagram

De betekenis van de kleuren is dat geel gekleurde applicatie componenten geen directe interface met de gebruiker hebben. De roze gekleurde applicatie componenten hebben dat wel. De grijs gekleurde applicatie componenten zijn niet-RWS systemen.

Direct valt op dat de SOLL situatie eenvoudiger is dan de IST situatie. CoastWatch, ERA en AMS worden nu ingevuld met één nieuw core systeem. Verder is de functie van de DIS overgenomen door de ADL die alle leveringen aan afnemende systemen doet. Dit leidt tot een opschoning van het applicatielandschap waardoor het beter te beheren is.
Er is ook een nieuw systeem in de SOLL ten opzichte van de IST: het NETPOS systeem dat GNSS correcties levert (AIS bericht 17).

De applicatie componenten zijn als volgt. Tevens wordt het verschil tussen de IST en de SOLL situatie gegeven.

AIS Base Station Een AIS Base Station zorgt voor de VHF communicatie met de schipper en ontvangt AIS berichten van alsmede levert AMS berichten aan de schipper. In de SOLL situatie levert het bovendien ook GNSS correcties aan de schipper. Tevens levert het Base Station metadata en monitoring data aan CoastWatch en het nieuwe core systeem in de IST respectievelijk SOLL situatie. Tenslotte kan het base station geconfigureerd worden door CoastWatch en het nieuwe core systeem in de IST respectievelijk SOLL situatie.

Partner DIS (alleen IST situatie) RWS krijgt niet alleen AIS berichten van haar eigen Base Stations maar heeft ook samenwerkingspartners met eigen Base Stations die via een partner DIS AIS berichten leveren. Het kan ook dat RWS AIS berichten van haar eigen base stations aan zo'n samenwerkingspartner via die partner DIS levert.

partner AIS systeem (alleen SOLL situatie) RWS krijgt niet alleen AIS berichten van haar eigen Base Stations maar heeft ook samenwerkingspartners met eigen Base Stations die via hun eigen systeem AIS berichten leveren. Deze worden geleverd aan het nieuwe core systeem, *niet* aan de ADL. Het kan ook dat RWS AIS berichten van haar eigen base stations aan zo'n partner systeem levert. Deze berichten komen van de ADL, *niet* van het nieuwe core systeem.

CoastWatch (alleen IST situatie) Dit is het centrale systeem in het Dutch Inland AIS Monitoring System (DIAMONIS). CoastWatch ontvangt AIS berichten van Base Stations en partner DIS systemen en distribueert ze via een DIS naar afnemers. Tevens kan CoastWatch AMS berichten naar Base Stations sturen. Tenslotte levert CoastWatch voor speciaal geconfigureerde regio's AIS berichten door aan ERA.

Core systeem (alleen SOLL situatie) Dit is een nieuw aan te schaffen COTS product dat het bestaande CoastWatch, ERA en AMS vervangt. In tegenstelling CoastWatch heeft het nieuwe core systeem wél een interface met de gebruiker want het wordt nu ook gebruikt voor het sturen van AMS berichten. De AMS berichten worden ook naar de ADL gestuurd die ze doorstuurt naar de AIS Historische Opslag en naar de SVV. De repeater functionaliteit wordt ook door het nieuwe core systeem geboden. En tenslotte gaat het nieuwe core systeem ook de GNSS correcties leveren aan de base stations (AIS bericht 17).

ERA (alleen IST situatie) Met de External Repeater Application (ERA) worden AIS berichten van base stations binnen een geconfigureerde regio heruitgezonden naar andere regio's. ERA krijgt hiervoor een AIS berichtenstroom van CoastWatch en filtert deze op regio en stuurt een deel van de berichten weer door naar CoastWatch om ze naar specifieke (andere) regio's te sturen.

DIS (alleen IST situatie) Een DIAMONIS Interface Server (DIS) distribueert AIS berichten verder naar afnemers. CoastWatch koppelt dus nooit rechtstreeks met een afnemer.

TMC systeem In verschillende Traffic Management Centers (TMC) staan systemen die de AIS berichten fuseren met radar data, de zogenaamde Radar AIS Fusion (RAF). In de IST situatie krijgt zo'n systeem nog de berichten van een DIS, in de SOLL situatie komen de berichten van de ADL.

Sluis/Brug systeem Op bedienposten van verschillende sluizen en bruggen staan systemen die de AIS berichten fuseren met radar data (RAF). In de IST situatie krijgt zo'n systeem nog de berichten van een DIS, in de SOLL situatie komen de berichten van de ADL.

ADL De AIS Distributie Laag (ADL) is door RWS in het leven geroepen om niet teveel DISsen te hoeven kopen maar om de data zelf te distribueren naar een groot aantal afnemers. In de IST situatie zijn dat: IVSNext, Vake, Dirkzwager, Euris, SVV, AIS Historische Opslag en de Provincie Zuid-Holland. In de toekomst ook een of meerdere olie- en gasexploitanten. In de SOLL situatie is de ADL hét systeem dat AIS berichten distribueert. Hiervoor heeft het één ingaande koppeling met het nieuwe core systeem en vele uitgaande koppelingen met de genoemde systemen maar ook met TMC systemen, sluis/brug systemen en met partner AIS systemen.

SVV De ScheepvaartVerkeersViewer (SVV) is een RWS applicatie die breed wordt toegepast op RWS locaties en ook op locaties van andere partijen dan RWS. Hier wordt het AIS beeld, zonder fusie met radar, in een webbrowser gepresenteerd om zo het overzicht te krijgen waar schepen zich bevinden. Op dit moment loopt er een onderzoek naar de toekomst van de SVV in het kader van het architectuurtraject Basis Op Orde. Kaartgeoriënteerd werken is voorzien in een nieuwe versie van de SVV en ook de in dit document genoemde trigger condities zullen hierin geïmplementeerd moeten worden.

AIS Historische Opslag Dit is het meest recente onderdeel van de AIS keten en doet wat de naam zegt: het opslaan en distribueren van AIS berichten. Er is geen verschil tussen IST en SOLL.

AMS (alleen IST situatie) De AIS Messaging Service (AMS) is het systeem waarmee een gebruiker bijvoorbeeld AtoN berichten kan broadcasten in een bepaald gebied. Hiervoor heeft AMS een gebruikersinterface en aan de andere kant een koppeling met CoastWatch.

NETPOS (alleen SOLL situatie) Het NETPOS systeem van het Kadaster is in staat GNSS correcties te leveren (AIS bericht 17). Deze worden geleverd aan het nieuwe core systeem.

Splunk SIEM (alleen SOLL situatie) Het Splunk SIEM systeem van het SOC ontvangt syslog events van Splunk agents op het nieuwe core systeem. Op basis van voorgedefinieerde regels in Splunk SIEM kunnen gebeurtenissen leiden tot een warning of emergency welke opgepakt en waarop geacteerd wordt door het SOC in combinatie met de beheerorganisatie van het nieuwe core systeem.

In het bovenstaande hebben we voor wat betreft de informatie vooral op het AIS bericht gefocust. Er zijn echter meer informatie artefacten zoals we in hoofdstuk 4.2 zagen. In de onderstaande tabel zien we in welke applicatie componenten de verschillende informatie artefacten gebruikt worden en welke component eigenaar is van het artefact:

	Base Station	CW (IST)	core (SOLL)	ERA (IST)	DIS (IST)	TMC SluisBrug	ADL	SVV	HO	AMS (IST)	NETPOS (SOLL)	Splunk (SOLL)	Opmerking
AIS bericht	**X**	X	**X**	X	X	X	X	X	X	**X**	**X**		core/AMS als AMS bericht NETPOS als GNSS correctie
Geaggregeerd AIS bericht							**X**	X	X				
GPS positie	**X**	X	X										
GNSS positie	**X**	X	X										
Radar beeld						X							Radar systeem is eigenaar
Regio			**X**	**X**									
Centrale configuratie		**X**	**X**	X	X					X			
Base station configuratie	X	**X**	**X**										
Status centraal systeem		**X**	**X**										
Status base station	**X**	X	X										
Alarm		**X**	**X**									X	
Conditie voor trigger								**X**					SOLL situatie
Conditie voor filter							**X**						
Statistieken		**X**	**X**										

Tabel 1: Component interaction view: Toekenning informatie artefacten aan applicatie componenten en eigenaarschap (vetgedrukt)

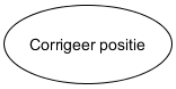
5.2.2 Applicatie scope

Zoals aangegeven in [AP-9] besteden we de core functionaliteit, die momenteel gerealiseerd wordt met de applicatie componenten CoastWatch, AMS en ERA, opnieuw aan.

5.2.3 Applicatie koppelvlakken

Uit de interacties tussen de applicatie componenten in Figuur 7 en Figuur 8 volgen de koppelvlakken.

De use cases getekend in de SOLL situatie worden als volgt gerealiseerd door de applicatie componenten en interacties (N.B. de lever, beheer en monitor use cases spreken voor zich en zijn niet beschreven):

Use case	**Component (interactie)**
	NETPOS → core systeem → AIS Base Station → schipper
	schipper → AIS Base Station → core systeem → ADL *of* schipper → partner AIS base station → partner AIS systeem → core systeem → ADL *of* Kustwacht/ Havenbedrijf Amsterdam/ Havenbedrijf Rotterdam/ Schelderadarketen partner AIS systeem → core systeem → ADL
	ADL
	ADL
	ADL
	schipper → AIS base station → core systeem → ander AIS base station → andere schipper

	Kustwacht → core systeem → AIS base station → schipper Verkeersbegeleider → core systeem → AIS base station → schipper
	ADL → RAF *of* ADL → SVV *of* ADL → IVSNext *of* ADL → Kustwacht/ TenneT/ Provincie Noord-Holland/ Euris/ Vake/ Dirkzwager/ Havenbedrijf Amsterdam/ Havenbedrijf Rotterdam/ Schelderadarketen partner systeem
	ADL → RAF → Verkeersbegeleider *of* ADL → RAF → Sluis/Brug operator *of* ADL → RAF → OEC medewerker *of* ADL → SVV → Verkeersbegeleider *of* ADL → SVV → Sluis/Brug operator *of* ADL → SVV → OEC medewerker
	ADL → RAF → Verkeersbegeleider *of* ADL → RAF → Sluis/Brug operator *of* ADL → RAF → OEC medewerker *of* ADL → SVV → Verkeersbegeleider *of* ADL → SVV → Sluis/Brug operator *of* ADL → SVV → OEC medewerker
	SVV → Verkeersbegeleider *of* SVV → Sluis/Brug operator *of* SVV → OEC medewerker
	RAF

	ADL → AIS Historische Opslag
	AIS Historische Opslag → WVL medewerker
	WVL medewerker

5.2.4 Beheer

Het applicatiebeheer is belegd bij CIV OSR SVM Services.

5.2.5 Kwaliteitseisen

Zie hoofdstuk 4.3.4.

6 Technische Architectuur

6.1 Specifieke technische kaders voor dit project

RWS werkt onder architectuur. Leidend zijn de architectuurprincipes (kaders). In dit hoofdstuk bekijken we de technische kaders en hoe zij van invloed zijn op de nieuwe AIS keten.
De omkaderde technische kaders zijn van toepassing:

[TIP-1] De technische infrastructuur van RWS is gericht op interoperabiliteit

[TIP-2] De technische infrastructuur van RWS ondersteunt rijksbrede samenwerking in publieke en private netwerken

[TIP-3] RWS richt zich op de kerntaken

[TIP-4] De RWS infrastructuur is flexibel, schaalbaar en efficiënt

[TIP-5] RWS meet kwaliteit en maakt management informatie inzichtelijk

[TIP-6] RWS maakt gebruik van gestandaardiseerde infrastructuur

Opmerking: [TIP-2] wordt al gedekt door [TIP-1].

	**TIP-1: De technische infrastructuur van RWS is gericht op interoperabiliteit**
Dit houdt in:	De RWS Technische infrastructuur is gericht op een samenhangende infrastructuur en een goede aansluiting op het applicatielandschap van zowel Rijkswaterstaat als partners.
Consequenties:	Door gebruik te maken van de standaard RWS infrastructuur wordt uitstekende bereikbaarheid tussen applicatie componenten onderling en tussen applicatie componenten en systemen van externe partijen nagestreefd. De basis hiervoor ligt in de standaard bouwblokken van IRN. Door RIVA bouwstenen Virtual Server Windows of Virtual Server Linux af te nemen hebben we geen zorgen over de hardware. Dit is dus een verandering ten opzichte van de huidige situatie waarbij de DIAMONIS core hardware beheerd wordt door de leverancier STV (als enige systeem in het ODC). Tenminste een eigen VPN zorgt voor afscherming en bescherming van de data en de connectiviteit. Door gebruik te maken van IPsec worden externe systemen/partijen in staat gesteld op een gestandaardiseerde en veilige manier connecties op te bouwen

	naar de systemen van RWS tegen de daarvoor geldende service levels.

<plaatje niet in PSA template>	**TIP-3: RWS richt zich op de kerntaken**
Dit houdt in:	De RWS Technische Infrastructuur wordt zo ingericht, dat RWS zich op de kerntaken kan richten en alles wat daarbuiten valt aan de markt kan worden overgelaten.
Consequenties:	Er wordt gebruik gemaakt van de standaard RIVA bouwstenen. De dienstverlening en het onderhoud van deze bouwstenen wordt aangeboden door marktpartijen zoals KPN, onder regie van RWS CIV IRN. Hierdoor kan RWS zich richten op haar kerntaken.

<plaatje niet in PSA template>	**TIP-4: De RWS infrastructuur is flexibel, schaalbaar en efficiënt**
Dit houdt in:	De RWS Technische Infrastructuur is flexibel, schaalbaar en efficiënt en kan daardoor omgaan met een veranderende Rijkswaterstaat en haar processen.
Consequenties:	Door voor het core systeem gebruik te maken van virtualisatie in combinatie met container techniek wordt de relatie tussen de applicatie componenten en de onderliggende infrastructuur minder groot waardoor de kwaliteitsaspecten flexibiliteit, schaalbaarheid en efficiëntie makkelijker te realiseren zijn. Voor het nieuwe core systeem eisen we dat het draait onder Kubernetes.

<plaatje niet in PSA template>	**TIP-5: RWS meet kwaliteit en maakt management informatie inzichtelijk**
Dit houdt in:	De RWS Technische Infrastructuur wordt beheerd op basis van meetbare kwaliteitscriteria en inzichtelijke management informatie.
Consequenties:	Door de gehele technische infrastructuur (netwerken, servers, OS'en en containers) af te nemen als RIVA bouwstenen zijn de service levels en kosten van te voren bekend en kan over de prestaties tijdens gebruikt gerapporteerd worden door RWS CIV IRN.

<plaatje niet in PSA template>	**TIP-6: RWS maakt gebruik van gestandaardiseerde infrastructuur**
Dit houdt in:	De infrastructuur bestaat uit gestandaardiseerde componenten die hergebruikt worden in de gehele organisatie.

Consequenties:	Dit zijn de RIVA bouwstenen waarvan ook AIS2025 gebruik zal maken.

6.2 Middleware, Platformen, Netwerkarchitectuur

6.2.1 Impact

De applicatie componenten van het IV systeem draaien op een groot aantal servers en op een groot aantal verschillende locaties.

Deze deployment view is hieronder gemodelleerd in de volgende UML *deployment diagrams* voor IST en SOLL. Hierbij is er voor de IST een knip gelegd waar de informatie de ADL binnengaat omdat de tekening anders te groot wordt.

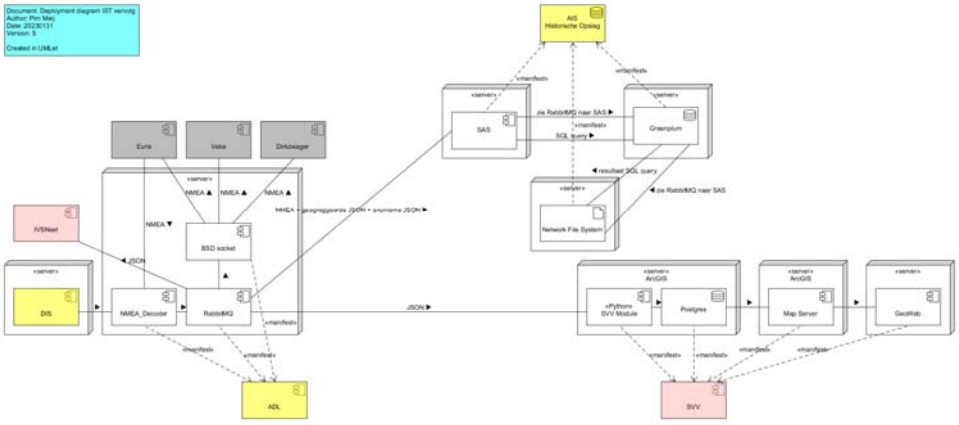
Opmerking: De getekende DIS servers zijn gebaseerd op het overzicht in [DIS accounts]. In de plaat zijn alleen DIS servers getekend die onderdeel uitmaken van productiesystemen, dus niet test systemen. Voor het volledige overzicht en meer details zie [DIS accounts].

Opmerking: In de eerste figuur zijn de 4 DISsen aan de linkerkant zowel leverend als afnemend. De overige DISsen in de figuur zijn alleen afnemend.

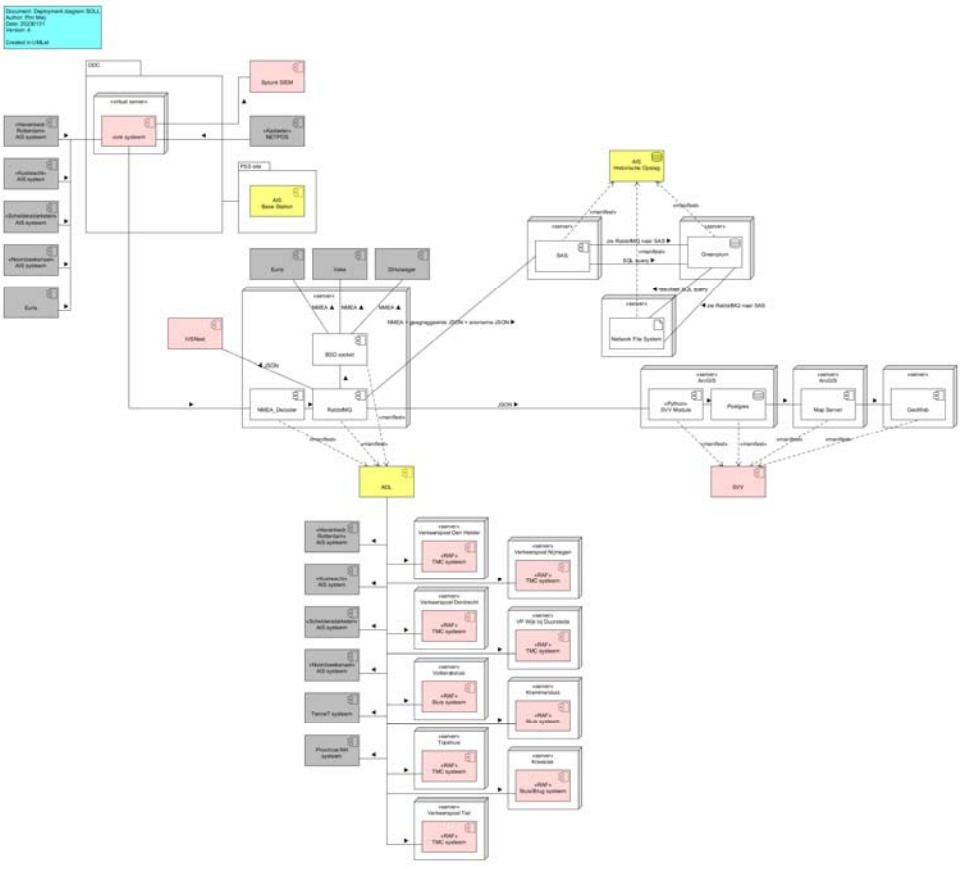
Opmerking: Soms is een applicatie component niet één component maar wordt er gebruikt gemaakt van verschillende zogenaamde middleware componenten. Tezamen vormen zij dan de functie van de applicatie component, of in UML termen zij ‘manifesteren’ zich als de applicatie component.



Figuur 9: AIS IST, Deployment view – Deployment diagram



Figuur 10: AIS IST, Deployment view – Deployment diagram vervolg



Figuur 11: AIS SOLL, Deployment view – Deployment diagram

AIS Base Station Er zijn vele AIS Base Stations in Nederland inland en op de Noordzee (58 in totaal op moment van schrijven). Iedere locatie waar een base station staat heet een Physical Shore Stations (PSS) alhoewel voor de nieuwe locaties op de Wind op Zee platformen deze naam de lading niet echt meer dekt.

CoastWatch (alleen IST situatie) Zie [DIAMONIS SDD]. De core systemen draaien in een redundante omgeving in de OverheidsDataCenters (ODC) AM4 en AM2. Er zijn drie AIS router servers (R1, R2, R3) en drie gateway servers (GW1, GW2, GW3). De router servers zijn verbonden met de base stations. De gateway servers zijn verbonden met de DISsen en de AMS server.

Core systeem (alleen SOLL situatie) Het nieuw aan te schaffen COTS product zal in het OverheidsDataCenter (ODC) draaien. In welk(e) ODC('s) en hoeveel virtuele servers er nodig zijn is nu niet bekend, dat zal moeten blijken uit de dimensionering die de marktpartij die het product zal leveren heeft berekend. Vanwege het missiekritieke karakter van de AIS keten is redundantie over twee ODC's waarschijnlijk nodig.

DIS (alleen IST situatie) Zie [DIAMONIS SDD]. Er zijn vele DISsen. Iedere toeleverancier van AIS gegevens heeft een DIS, het gaat om de locaties Noordzeekanaal (Havenbedrijf Amsterdam), Schelde Radar Keten, Kustwacht en Havenbedrijf Rotterdam. Voor Schelde Radar Keten (SRK) staat de DIS in het ODC. Ook voor iedere afnemer wordt een DIS gebruikt, het gaat om de TMC locaties Dordrecht, Tiel, Nijmegen en Neeltje Jans, en om de sluizen Volkerak, Krammer en Kreekrak. Tenslotte is er ook een DIS in het ODC waarop de ADL is aangesloten.

TMC systeem Op de TMC locaties staan applicaties die Radar AIS Fusion doen.

Sluis/Brug systeem Op de sluizen en een keer op een brug staan eveneens applicaties die de Radar AIS Fusion doen.

ADL De ADL is een samenwerking van een aantal componenten:

- **NMEA_Decoder** Deze component decrypt de van de DIS ontvangen NMEA berichten en zet ze op de RabbitMQ. Tevens ontvangt de NMEA_Decoder in de IST situatie NMEA berichten van de (niet-RWS) Euris applicatie, in de SOLL situatie is het niet langer gewenst dat Euris direct aan de ADL levert en zal dit via het core systeem moeten.

- **RabbitMQ** Deze component ontvangt de decrypted NMEA berichten van de NMEA_Decoder en biedt ze aan middels een queue als JSON aan IVSNext en als JSON aan de SVV. Tevens worden ze aangeboden aan een Berkely (BSD) socket. Tenslotte worden er NMEA, geaggregeerde JSON en anonieme JSON aangeboden aan de AIS Historische Opslag.

- **BSD Socket** Deze component ontvangt NMEA berichten (haalt ze op in technische zin) van de RabbitMQ en stuurt ze door naar verschillende externe partijen: Euris, Vake en Dirkzwager.

De SOLL situatie toont de centrale plaats die de ADL gaat innemen. Hoe bestaande afnemers (externe partijen, TMC locaties, sluizen en bruggen) gaan afnemen is nu niet aangegeven. Dit kan via de getekende BSD socket of via de RabbitMQ maar dit zal tijdens de migratie in overleg met de afnemers bepaald moeten worden.

SVV De SVV is een samenwerking van een aantal middleware componenten:

- **SVV Module** Dit is een Python applicatie die connecteert naar de ADL en als functie heeft het verwerken van de JSON datastroom op basis van geografische kenmerken en het bijwerken van de database (*insert* of *update*).
- **Postgres** De database.

- **Map Server** De resultaten die in de database waren opgeslagen worden verwerkt tot meerdere map services. In het geval van SVV wordt er gebruik gemaakt van een event processor, in de vorm van ArcGIS Geo Event, en een map service generator, op basis van ArcMap.
- **GeoWeb** Dit is de viewer die uiteindelijk de resultaten aan de gebruiker presenteert.

AIS Historische Opslag De AIS Historische Opslag is een samenwerking van een aantal middleware componenten:

- **SAS** Het SAS platform haalt NMEA, geaggregeerde JSON en anonieme JSON van de RabbitMQ. Deze berichten worden bewaard in de Greenplum. Ook kan de gebruiker via SAS queries uitvoeren, deze worden als SQL query doorgezet naar de Greenplum.
- **Greenplum** De Greenplum is voor de short term storage van NMEA, geaggregeerde JSON en anonieme JSON. Tevens voert de Greenplum SQL queries uit en worden de resultaten in de NFS weggeschreven. Periodiek wordt ook de short term storage weggeschreven naar de NFS.
- **Network File System** De long term storage. Tevens krijgt een gebruiker na een query een adres op de NFS om de resultaten van de query op te halen.

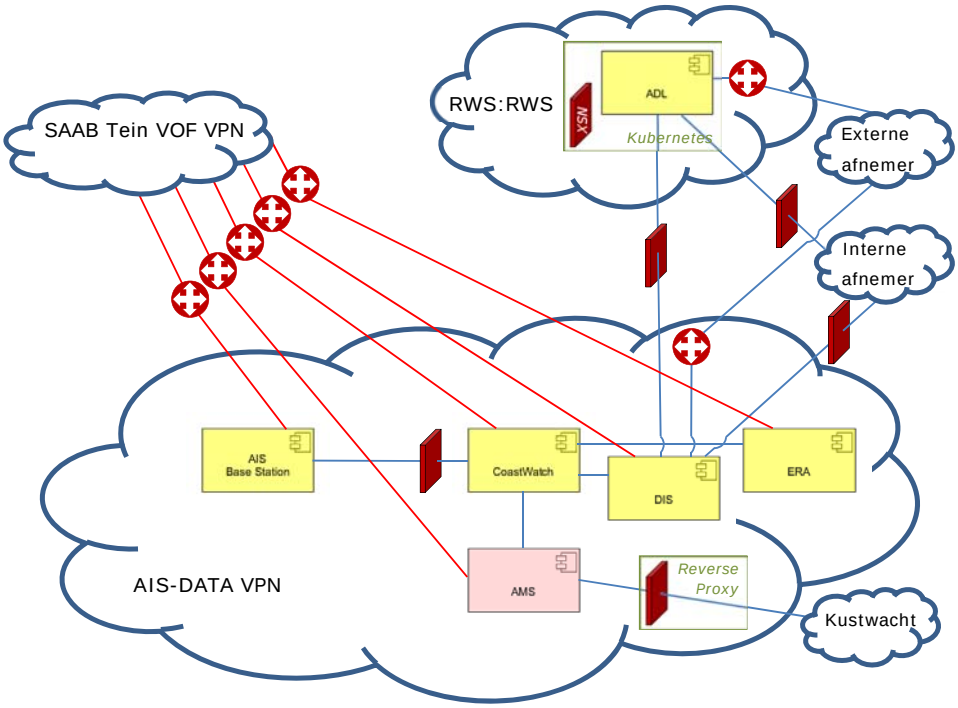
AMS (alleen IST situatie) De AIS Messaging Service (AMS) is het systeem waarmee een gebruiker diverse AIS gerelateerde berichten kan sturen aan een schipper. Hiervoor heeft AMS een gebruikersinterface en aan de andere kant een koppeling met CoastWatch.

NETPOS (alleen SOLL situatie) Het NETPOS systeem van het Kadaster levert GNSS correcties aan het nieuwe core systeem.

Splunk SIEM (alleen SOLL situatie) Het Splunk SIEM systeem van het SOC ontvangt relevante syslog events van Splunk agents op het nieuwe core systeem.

6.2.2 Technische koppelvlakken

In onderstaande figuur (geen UML) is de huidige zonering aangegeven voor AIS.



Figuur 12: AIS IST, Zonering

Iedere wolk stelt een Virtual Private Network (VPN) voor. Rijkswaterstaat maakt veelvuldig gebruik van VPN's: gescheiden compartimenten binnen het grote NNV die alleen door opengestelde firewalls met elkaar kunnen communiceren.

Een RWS VPN is standaard een multi point virtueel laag 3 netwerk, geïsoleerd van andere RWS VPN's. Toegang kan verkregen worden vanuit het ene RWS VPN naar het andere via de centrale firewall. Elk RWS VPN is voorzien van zo'n firewall.

De blauwe lijnstukken geven wederom de functionele datastroom aan. De rode lijnstukken geven het beheer aan.

Alles wat AIS productie is, staat in het AIS-DATA VPN. Dit geldt zowel voor de Base Stations, CoastWatch, de DISsen, ERA als AMS. Wel is het zo dat er een firewall zit tussen de buiten geplaatste Base Stations en het in het ODC geplaatste CoastWatch.

SAAB Tein VOF heeft middels IPsec koppelingen via Internet en een Gateway toegang vanaf hun eigen VPN tot het AIS-DATA VPN. In de koppeling is een groot aantal firewall regels gedefinieerd zodat SAAB Tein VOF alle verschillende instanties van de applicatie componenten kan bereiken. Deze oplossing wordt tegenwoordig niet meer geleverd vanuit RWS door KPN.

De interne afnemers van een DIS hebben een firewall opening om vanuit hun eigen VPN naar het AIS-DATA VPN te communiceren.

De externe afnemers van een DIS hebben middels een IPsec koppeling via Internet en een Gateway toegang vanaf hun eigen VPN tot het AIS-DATA VPN. Als de afnemer ook leverancier is dan wordt dezelfde koppeling gebruikt.

Opmerking: Voor TenneT die AIS berichten afneemt van Noordzee base stations is de situatie iets anders. Zij hebben een vaste externe toegangsvoorziening in plaats van een IPsec koppeling via Internet. Dit detail is niet getekend in de plaat.

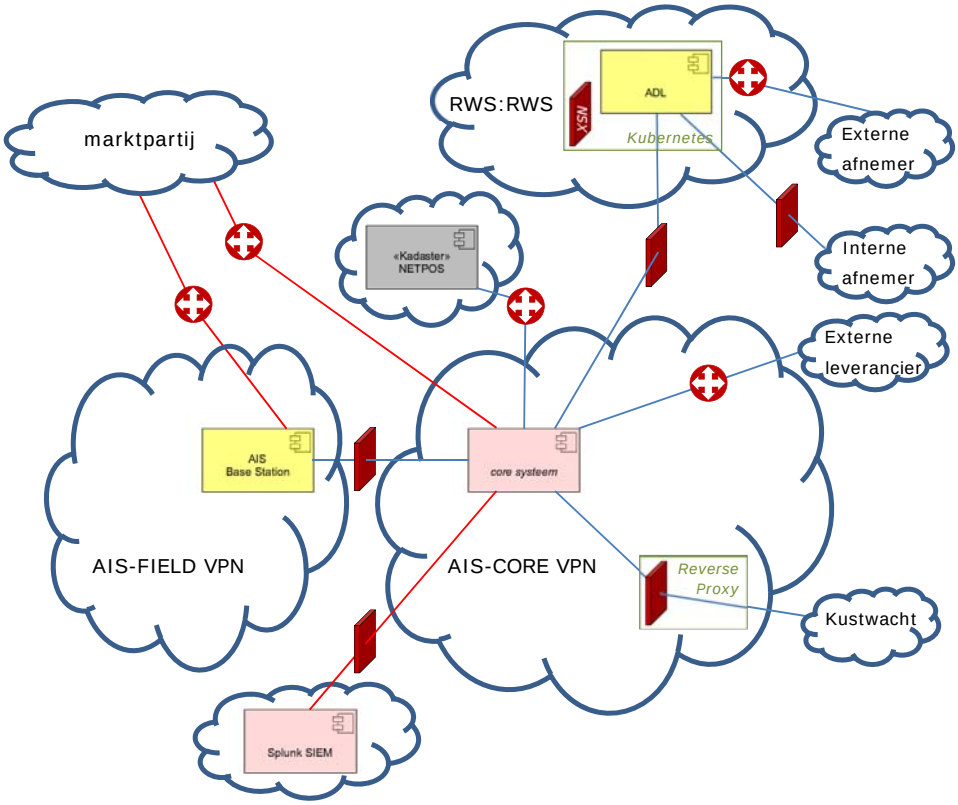
ADL draait in het RWS:RWS VPN en communiceert, uiteraard ook weer via een firewall, met de DIS. ADL draait in een Kubernetes container en de virtuele VMware server waarop de Kubernetes container draait is ook weer afgeschermd met een zogenaamde NSX firewall.

De interne afnemers van ADL hebben een firewall om vanuit hun eigen VPN naar het RWS:RWS VPN te communiceren en een regel op de genoemde NSX firewall.

De externe afnemers van ADL hebben middels een IPsec koppeling via Internet en een Gateway toegang vanaf hun eigen VPN tot het RWS:RWS VPN.

De Kustwacht heeft via een reverse proxy toegang tot de AMS web client. Hiervoor is de Kustwacht gewhitelist op de firewall van de proxy. De Kustwacht maakt gebruik van een Rijksweb URL.

In onderstaande figuur (geen UML) is de mogelijk toekomstige zonering aangegeven voor AIS.



Figuur 13: AIS SOLL, Zonering

In tegenstelling tot de IST situatie is de “buitenboel” nu gescheiden van het ODC: de Base Stations en het core systeem bevinden zich in het AIS-FIELD VPN en het AIS-CORE VPN respectievelijk (de namen zijn indicatief). Er is wederom een firewall tussen de Base Stations en het core systeem.

De marktpartij die het beheer gaat doen heeft middels IPsec koppelingen via Internet en een Gateway toegang vanaf hun eigen VPN tot het AIS-FIELD VPN en het AIS-CORE VPN.

ADL draait nog steeds in het RWS:RWS VPN in een Kubernetes container waarbij de virtuele VMware server waarop de Kubernetes container draait is afgeschermd met een NSX firewall.

De interne afnemers van ADL hebben wederom een firewall om vanuit hun eigen VPN naar het RWS:RWS VPN te communiceren en een regel op de genoemde NSX firewall.

De externe afnemers van ADL hebben wederom middels een IPsec koppeling via Internet en een Gateway toegang vanaf hun eigen VPN tot het RWS:RWS VPN.

De externe leveranciers aan het core systeem hebben ook middels een IPsec via Internet en een Gateway toegang vanaf hun eigen VPN tot het AIS-CORE VPN.

De Kustwacht heeft via een reverse proxy toegang tot het core systeem ten behoeve van de web client die de AMS functionaliteit verzorgt.

Er is verbinding tussen de NETPOS server van het Kadaster en het core systeem middels een IPsec koppeling via Internet en een Gateway.

Tenslotte is er via een firewall verbinding tussen het core systeem en het bij het SOC gehuisveste Splunk SIEM.

6.2.3 Technische scope

De volgende RIVA bouwstenen worden gebruikt, hierbij wordt de terminologie van de RIVA van Architecture Building Block (ABB) en Solution Building Block (SBB) aangehouden.

Architecture Building Block	**Solution Building Block**	**Gebruik**
Externe (Web)Applicatie connectiviteit	Reverse Proxy	Voor toegang van de Kustwacht tot de web client voor het versturen van AMS berichten.

Locatiegebonden Netwerk Toegang door Derden	IPsec koppeling via Internet	Voor beheertoegang van een marktpartij tot het nieuwe core systeem en de Base Stations. Voor systemen van externe partners die AIS berichten leveren aan het nieuwe core systeem dan wel afnemen van de ADL. Eveneens voor de koppeling met het NETPOS systeem van het Kadaster.
Locatiegebonden Netwerk Toegang door Derden	Vaste externe toegangsvoorziening	Voor beheertoegang van een marktpartij tot het nieuwe core systeem en de Base Stations. Voor systemen van externe partners die AIS berichten leveren aan het nieuwe core systeem dan wel afnemen van de ADL. Eveneens voor de koppeling met het NETPOS systeem van het Kadaster.
Logging beveiligingsmeldingen	Splunk Enterprise Security	Voor het monitoren van het nieuwe core systeem.
Container as a Service	Kubernetes ODC	Platform as a Service (PAAS) voor het draaien van de ADL (bestaande situatie) en het nieuwe core systeem.
Big Data opslag	Greenplum	Voor de AIS Historische Opslag (bestaande situatie).
Virtual Server	Windows	OS voor het nieuwe core systeem.
Virtual Server	Linux	OS voor het nieuwe core systeem.
Bestandsopslag	NFS	Voor de AIS Historische Opslag (bestaande situatie).

Netwerkcompartiment	VPN	Voor het nieuwe core systeem en voor de bestaande en toekomstige base stations.
Inter compartiment	VPN Firewall	Tussen de RWS VPN's onderling.

Opmerking: Om praktische redenen wordt niet de hele RIVA-lijst hier gekopieerd maar alleen de RIVA bouwstenen die gebruikt gaan worden zijn genoemd. Voor de hele RIVA-lijst zie [RIVA].

Opmerking: Of gebruik gemaakt wordt van een IPsec koppeling of een vaste voorziening is een afweging van geld en kwaliteit. Een vaste voorziening is betrouwbaarder maar ook duurder.

6.2.4 Beheer

Het technisch beheer is belegd bij CIV OSR SVM Services TAB-SVM. Eventueel wordt een marktpartij ingeschakeld om onder regie van TAB-SVM het technisch beheer te doen. De 1e lijn is dan MKO, de 2e lijn is TAB-SVM en de 3e lijn is de marktpartij.

6.2.5 Kwaliteitseisen

Aangezien AIS als missiekritiek is bestempeld betekent dit een service window van 24x7 en hersteltijd van < 4 uur.

Voordat een (nieuwe) release van het nieuwe core systeem in productie gaat, dient er acceptatie plaats te vinden. Dit betekent dat het core systeem getekend in Figuur 11 en Figuur 13, in welke verschijningsvorm dit dan ook zal zijn, een dubbele deployment moet hebben: een keer in de acceptatieomgeving en een keer in de productieomgeving.
Omdat het core systeem een COTS product zal zijn, is het logisch om de ontwikkel- en testomgeving bij de leverancier te laten.

7 Beveiliging

7.1 Specifieke beveiligingskaders voor dit project

RWS werkt onder architectuur. Leidend zijn de architectuurprincipes (kaders). In dit hoofdstuk bekijken we de beveiligingskaders en hoe zij van invloed zijn op de nieuwe AIS keten.
De omkaderde beveiligingskaders zijn van toepassing:

[SP-1] Beveiliging op basis van risicoafweging

[SP-2] Beveiliging is uit diverse lagen opgebouwd

[SP-3] Beveiliging zo dicht mogelijk bij te beveiligen asset

[SP-4] Beveiliging is ongecompliceerd

[SP-5] Beveiliging is makkelijk in gebruik

[SP-6] Beveiligingsincidentdetectie is geborgd

[SP-7] Incidentresponse is geborgd en geoefend

[SP-8]Een IA object is aantoonbaar beveiligd

Opmerking: [SP-4] is niet van toepassing. Dat wil niet zeggen dat de beveiliging gecompliceerd is maar het nieuwe core systeem wordt een COTS product en dit wordt *as is* ingekocht en volgens de gebruikelijke praktijk van fysieke beveiliging en zonering en afscherming, zie hoofdstuk 6.2.2, beveiligd.

	**SP-1: Beveiliging op basis van risicoafweging**
Dit houdt in:	Eisen voor beschikbaarheid, integriteit en vertrouwelijkheid afgeleid van expliciete risicoafweging in de keten.
Consequenties:	Op basis van een BIO toets inclusief een Risico Impact Analyse (RIA) moeten de beveiligingsmaatregelen per applicatie component worden bepaald om de vertrouwelijkheid, integriteit en beschikbaarheid van de informatie te garanderen. De bestaande RIA wordt geactualiseerd.

	**SP-2: Beveiliging is uit diverse lagen opgebouwd**
Dit houdt in:	Restrisico's van maatregelen worden verminderd door aanvullende maatregelen te treffen. Preventief en reactief.
Consequenties:	Er moeten per applicatie component meerdere lagen van beveiliging worden toegepast. De fysieke beveiliging zal altijd geborgd moeten zijn door de locatie waar de component gehuisvest is en wordt aangevuld met multi factor authenticatie. Reactief zal er zowel fysiek als digitaal op anomalieën moeten worden gemonitord. Multi factor authenticatie gebeurt nu ook al: bijvoorbeeld SAAB heeft in de IST situatie een username en password nodig én dient fysiek aanwezig te zijn op hun kantoor in Amstelveen om CoastWatch en de base stations te beheren.

	**SP-3: Beveiliging zo dicht mogelijk bij te beveiligen asset**
Dit houdt in:	Door de maatregelen dicht bij de te beschermen assets te plaatsen, blijft de omvang van te beschermen assets beperkt.
Consequenties:	Daar waar mogelijk zal op individuele assets worden beveiligd. Er zal altijd een vorm van fysieke beveiliging moeten zijn. Voor nieuw aan te schaffen base stations kan gedacht worden aan standaard encryptie van de harde schijven. Dit kan tegenwoordig automatisch en levert geen tijdsvertraging op.

	**SP-5: Beveiliging is makkelijk in gebruik**
Dit houdt in:	Veilig werken moet eenvoudig zijn voor medewerkers en IV beheerders, anders omzeilen zij de securitymaatregelen.
Consequenties:	Er moet een balans zijn tussen een eenvoudige AIS keten enerzijds en eisen vanuit de BIO, de RIA en de IRN PDC's.

	**SP-6: Beveiligingsincidentdetectie is geborgd**
Dit houdt in:	Als een security incident optreedt, kan de aanval en de impact alleen worden ingeperkt als het incident wordt ontdekt.

Consequenties:	Het digitaal op anomalieën monitoren dient te gebeuren met behulp van de RIVA bouwsteen Splunk Enterprise Security. Bovendien maken we gebruik van het RWS netwerk wat standaard al op anomalieën controleert.

	**SP-7: Incidentresponse is geborgd en geoefend**
Dit houdt in:	Als een security incident wordt ontdekt, moet de organisatie geoefend zijn in het inperken van de aanval en de impact.
Consequenties:	Er moet een beveiligingsplan komen inclusief backup en recovery. We kiezen net als in de IST situatie voor het nieuwe core systeem een active-active oplossing die op regelmatige basis getest wordt.

7.2 Beveiligingsmiddelen en maatregelen

7.2.1 Impact

Er komt een koppeling van de AIS keten, gezien de projectscope dus vanaf het nieuwe core systeem, naar Splunk SIEM aan de kant van het Security Operations Center (SOC).

7.2.2 Beveiliging scope

In de SOLL situatie doet het SOC monitoring met behulp van Splunk SIEM voor het detecteren van security incidenten. Op basis van relevante logging informatie van verschillende Splunk agents op Windows en/of Linux servers van het nieuwe core system kan het SOC met behulp van Splunk SIEM een security trail maken. Dit omvat gegevens ten aanzien van netwerkbelasting en het ontvangen, verwerken en verzenden van data, welke gebruikers ingelogd hebben op het systeem alsmede belangrijke OS en apparatuur gebeurtenissen. Er wordt gebruik gemaakt van de security levels warning en emergency.

7.2.3 Beveiliging koppelvlakken

Er komt een koppeling tussen het nieuwe core AIS-CORE VPN en het Splunk Siem systeem. De syslog server is de door het SOC geprefereerde methode om een koppeling te maken met Splunk SIEM.
Overigens controleert het Splunk SIEM al in de huidige situatie op anomalieën in het RWS netwerk.

7.2.4 Beheer

Het beveiligingsbeheer wordt belegd bij de applicatiemanager daarbij ondersteund door het SOC.

7.2.5 Kwaliteitseisen

Beveiliging dient 24/7 te zijn.

8 Industriële Automatisering

Industriële automatisering is voor AIS niet van toepassing en dit hoofdstuk is daarom niet ingevuld.

Bijlage Appendices

A.1 Referenties

Normatieve referenties

iAIS-CCNR 1.01	Vessel Tracking and Tracing Standard for Inland Navigation, Central Commission for Navigation on the Rhine, versie 1.01, 10 oktober 2007
iAIS-CCNR 1.2	Vessel Tracking and Tracing Standard for Inland Navigation, Central Commission for Navigation on the Rhine, versie 1.2, 23 april 2013
ITU-R M.1371-4	Recommendation ITU-R M.1371-4, “Technical characteristics for an automatic identification system using time division multiple access in the VHF maritime mobile frequency band”, International Telecommunications Union, april 2010
ITU-R M.1371-5	Recommendation ITU-R M.1371-5, “Technical characteristics for an automatic identification system using time division multiple access in the VHF maritime mobile frequency band”, International Telecommunications Union, februari 2014
US AIS2025	User stories AIS2025, Rijkswaterstaat CIV, versie 1.0 (Definitief) van 22 november 2022
RIVA	Rijkswaterstaat IV aansluitvoorwaarden, vigerende versie op moment van opstellen PSA, te vinden op https://werkwijzerrws.intranet.rws.nl/index2.html en zoek op ‘RIVA’
VEK	Vastgestelde Enterprisearchitectuurkaders (http://corporate.intranet.rws.nl/Organisatie/Processen/Informatievoorziening/Inrichting_proces/Besturen_van_IV/Architectuur/Enterprisearchitectuur/Vastgestelde_Enterprisearchitectuurkaders/)
PID AIS 2025	Projectinitiatiedocument Vooronderzoek AIS 2025, Rijkswaterstaat CIV, versie 0.3 (Concept), juli 2022
PvA AIS Next	Plan van Aanpak Vooronderzoek AIS Next, Rijkswaterstaat CIV, versie 0.6 (Concept) van 28 september 2022
Standaarden	Onderzoek relevante standaarden in het kader project AIS 2025, Rijkswaterstaat CIV, versie 1.0 (Definitief) van 12 oktober 2022

Informatieve referenties

DIAMONIS SDD	DIAMONIS System Design Description, RWS, versie 1.0, 22 juni 2015
DIAMONIS SSS	DIAMONIS System/Subsystem Specification, RWS, versie 1.0.7 (Author approved), 23 juni 2015
DIS accounts	DIS_accounts_info.xlsx, bestand gekregen van Corstiaan Mulckhuijse (Rijkswaterstaat CIV) op 8 november 2022
IMO Circ.236	Guidance on the Application of AIS Binary Messages (SN/Circ.236), International Maritime Organization, 28 mei 2004
IMO Circ.289	Guidance on the use of AIS Application-Specific Messages (SN.1/Circ.289), International Maritime Organization, 2 juni 2010
IRS ADL	IRS AIS Distributie Laag, IRS ADL, RWS, 14 december 2020
PIA	Gegevensbeschermingseffectbeoordeling (PIA), Operationeel Scheepvaartverkeersmanagement (PIA-SVM-O), RWS, versie 1.0 (Definitief) van 2 december 2019
Scenariokeuze	Memo Scenariokeuze Vooronderzoek AIS2025, RWS CIV, versie 1.0 (Definitief) van 22 november 2022
UML	https://www.uml.org/

A.2 Afkortingen en acroniemen

AIS	Automatic Identification System
AMS	AIS Messaging Service
BSD	Berkeley Software Distribution
COTS	Commercial Off The Shelf
ETA	Estimated Time of Arrival
GNSS	Global Navigation Satellite System
IPsec	Internet Protocol security
MMSI	Maritime Mobile Service Identity
NOGEPA	Nederlandse Olie en Gas Exploratie en Productie Associatie
PSS	Physical Shore Station
RTA	Requested Time of Arrival
SSL	Secure Sockets Layer
STV	SAAB Tein VOF
TLS	Transport Layer Security
UML	Unified Modeling Language