

Digitaliseren Inventory of Hazardous Materials

Joris Elfferich 1013457

Docenten: Lisa Weggemans, Anthony Bernadina

10 juni 2024



Voorwoord

Na een geweldige en avontuurlijke minor af gerond te hebben in Taiwan begon ik in Februari met deze afstudeerstage. Eenmaal teruggekeerd naar mijn Nederlandse leven heb ik met doorzettingsvermogen en enkele tegenslagen na vier maanden deze scriptie afgerond. Ik vond het een leuke periode, en de opdracht een interessant onderwerp om over te leren. Wel vind ik het jammer dat mijn studietijd bij de hogeschool Rotterdam ten einde is.

Eerst wil ik mijn begeleider Frederik de Wit bedanken voor zijn waardevolle begeleiding bij dit onderwerp, hulp met het definiëren en uitvoeren van de opdracht en natuurlijk zijn steun tijdens dit project.

Daarnaast wil ik ook mijn dankbaarheid uiten aan Lisa Weggemans en Anthony Bernadina, voor de goede feedback die mij heeft geholpen het eindproduct stukken beter te maken.

Het schrijven van deze scriptie heeft mij meer ervaring opgeleverd in het uitvoeren en uitschrijven van onderzoek, en in het beter leren werken met LaTeX. Omdat dit onderzoek een van de eerste is over het gebruik van blockchain voor het beheren van de IHM, hoop ik dat er meer onderzoek en implementaties zullen volgen in de maritieme wereld om zo de waarborging van de IHM te verbeteren.

Joris Elfferich

Delft

13/05/24

Samenvatting

Digitalisering kan de waarborging van de Inventory of Hazardous Materials (IHM) aanzienlijk verbeteren door verschillende huidige problemen op te lossen. Momenteel is er geen manier om de betrouwbaarheid van de informatie te achterhalen, versiebeheer is vaak niet goed aanwezig, de documentopslag is vaak niet veilig en toegang tot documenten is onhandig voor de stakeholders. Digitalisering biedt oplossingen op al deze problemen: documenten kunnen onveranderlijk worden gemaakt na goedkeuring, een versiebeheer kan automatisch worden bijgehouden, documenten worden veilig opgeslagen op een server, en stakeholders kunnen gemakkelijke krijgen toegang via een accountmanagementsysteem en een schipmodule.

De digitalisering van de IHM beïnvloedt veel stakeholders zoals scheepsbouwers, leveranciers, scheepseigenaren, classificatiemaatschappijen, havenautoriteiten en IHM-experts. Een gecentraliseerde webinterface verbetert de samenwerking tussen deze partijen. Classificatiemaatschappijen kunnen documenten goedkeuren, scheepseigenaren beheren en uploaden nieuwe versies, en andere stakeholders hebben alleen toegang om documenten te bekijken.

Voor veilige opslag wordt een private blockchain gebruikt, die onveranderlijkheid en transparantie garandeert. Deze blockchain werkt door data in opeenvolgende blocks te linken en op te slaan, met hashes die de integriteit van de data controleren. Dit systeem is erg veilig en overzichtelijk. De bestanden worden veilig binnen de blockchain opgeslagen, met menselijke goedkeuring voor elke nieuwe toevoeging. Na het uploaden kunnen er geen details binnen het document meer worden aangepast.

Een schip module koppelt de IHM aan een schip, hierop kan de blockchain via een app op een smartphone worden uitgelezen via bluetooth. Deze module maakt verbinding met de blockchain server via LoRa, een kosteneffectieve draadloze techniek die grote afstanden kan overbruggen. De gekozen microcontroller,

de Heltec Wireless Tracker, heeft ingebouwde Bluetooth en LoRa modules. Waardoor de schip module erg compact is. Er wordt vervolgens een antenne gebruikt voor het ontvangen van LoRa signaal die buiten op het schip wordt gemonteerd.

Door al deze eigenschappen wordt de naleving van de IHM-certificering aanzienlijk verbeterd. De betrouwbaarheid wordt gewaarborgd door het onveranderlijke maken van de documenten via blockchain, goedkeuring van de relevante stakeholder is vereist voor uploaden van data, versiebeheer wordt hierbij ook automatisch bijgehouden, de documenten worden veilig opgeslagen op een cloud server, en toegang tot documenten is via een gedeelde webinterface en een schip module goed geregeld. Deze digitaliseringstechnologieen zijn dus enorm waardevol om zo de naleving van de certificering van de IHM te beheren.

Inhoudsopgave

1 Bedrijf	4
2 Inleiding	4
3 Theoretisch kader	6
3.1 Definitie IHM	6
3.2 Definitie digitalisering en verbetering	6
3.3 Beïnvloeding stakeholders	7
3.4 Begrippen voor het digitaal beheren van data	7
3.5 Begrippen voor de implementatie van de schip module	8
4 Methodologie	10
5 Resultaten	11
5.1 Wat zijn de verbeterpunten die alleen door digitalisering de IHM waarborging verbeteren?	11
5.2 Hoe worden verschillende stakeholders beïnvloed door de digitalisering van de IHM	13
5.3 Hoe wordt de IHM digitaal beheerd in een veilige omgeving??	15
5.4 Hoe wordt de IHM gekoppeld aan een schip?	18
5.5 Hoe wordt een simpele gebruikersomgeving rondom de digitale omgeving gemaakt?	22
6 Conclusie	25
6.1 Dit zijn de verbeterpunten die door digitalisering de IHM waarborging verbeteren.	25
6.2 Zo worden verschillende stakeholders beïnvloed door de digitalisering van de IHM.	25
6.3 Zo wordt de IHM digitaal beheerd in een veilige omgeving.	26
6.4 Zo wordt de IHM gekoppeld aan een schip.	26
6.5 Zo wordt een simpele gebruikersomgeving rondom de digitale omgeving gemaakt.	26
6.6 Hoe kan de naleving van de certificering van de IHM op schepen worden gewaarborgd en verbeterd met behulp van digitalisering technologieën?	27
7 Aanbevelingen	28
8 Bronnen	29
9 Bijlage	31
9.1 Progress Flow	31

1 Bedrijf

Center of Expertise HRTech is een samenwerkingspartner op het gebied van praktijkgericht onderzoek voor het duurzaam inzetten van grondstoffen en energie in het haven industrieel complex van Rotterdam. Als Centre of Expertise (CoE) van Hogeschool Rotterdam is het de verbindende schakel tussen onderzoek, onderwijs, overheid, ondernemers en omgeving. Met verschillende lectoraten heeft het gedegen kennis in huis en met hen netwerk brengen ze partijen uit allerlei sectoren samen in de vorm van publiek private samenwerkingen. Binnen al deze programma's staat de verbinding tussen leren, werken en innoveren centraal.

Enkele onderzoeksrichtingen waar CoE HRTech aan werkt zijn:

1. Verduurzaming van Energie en Industrie
2. Slimme Logistiek en Maritieme Innovatie
3. Duurzame Stedelijke Delta.

2 Inleiding

De Hong Kong Internationale Conventie voor het Veilig en Milieuverantwoord Recyclen van Schepen heeft "The Inventory of Hazardous Materials" (IHM) geïntroduceerd. Dit door groeiende zorgen over de milieugevolgen en veiligheid bij de scheepsrecyclingindustrie. De IHM is een document dat informatie bevat over schadelijke materialen aan boord. Nu ligt er meer verantwoordelijkheid bij de scheepseigenaren voor het onderhouden van de IHM. Het belang van de IHM komt vooral naar voren wanneer een schip wordt afgedankt of gerecycled. De aanwezigheid van gevaarlijke materialen aan boord kan namelijk significantie milieu- en gezondheidsrisico's met zich meebrengen tijdens het sloopproces. Daarom is het belangrijk dat recyclingfaciliteiten toegang hebben tot nauwkeurige en actuele informatie over deze materialen. Dit stelt hen in staat om de nodige voorzorgsmaatregelen te nemen tijdens het recyclen. Sommige scheeps-eigenaren zouden informatie kunnen aanpassen of weglaten in het IHM om recyclingskosten voor zichzelf te besparen. Zo kunnen ze proberen te voorkomen dat ze moeten betalen voor het veilig recyclen of verwijderen van gevaarlijke materialen. Dit kan voor ernstige consequenties zorgen, omdat gevaarlijke materialen mogelijk niet op een verantwoorde en veilige manier worden behandeld en verwijderd. Dit kan leiden tot ernstige milieuproblemen, voor waterwegen en het ecosysteem, en potentiële gezondheidsrisico's voor mens en dier die worden blootgesteld aan deze gevaarlijke stoffen. Daarom is het van cruciaal belang dat er toezicht wordt gehouden op de naleving van de IHM en er streng wordt opgetreden tegen pogingen tot manipulatie of misbruik van dit document.

De "EU Ship Recycling Regulation" is op 31 december 2020 in gegaan en is van toepassing op elk schip van 500 GT (Gross tonnage) of meer dat een EU-haven of ankerplaats aandoet (ongeacht de vlag). Schepen moeten nu dus een geldige en gecertificeerde IHM aan boord hebben om aan te meren binnen Europa. Dit om het dragen van een IHM een vereiste te maken om zo de scheepsrecycling te bevorderen.

Op dit moment is de IHM een (uitgeprint) pdf document dat frequent van eigenaar veranderd, dit is niet erg veilig of betrouwbaar. De beste oplossing zou dit document on aanpasbaar maken en een goed versiebeheer opstellen. Het document moet nog wel inzienbaar zijn voor de andere stakeholders die dan ook kunnen kijken of de informatie klopt, maar ze mogen de IHM niet aanpassen. Met een stukje papier of een onbeveiligd elektronisch document gaat dit moeilijk, dus daarvoor is een betere

digitale oplossing nodig. Met digitale toevoegingen zoals een goed versiebeheer, verschillende accounts voor de stakeholders en de IHM onveranderlijk te maken na het uploaden kan de IHM zo een stuk beter worden gewaarborgd. Alleen welke digitaliseringstechnologieën worden hierbij gebruikt? Om dit te beantwoorden komt de onderzoeksvraag ten stand:

Hoe kan de naleving van de certificering van de IHM op schepen worden gewaarborgd en verbeterd met behulp van digitaliseringstechnologieën?

Om de hoofdvragen te beantwoorden zijn de volgende deelvragen opgesteld:

1. Wat zijn de verbeterpunten die alleen door digitalisering de IHM waarborging verbeteren?
2. Hoe worden verschillende stakeholders beïnvloed door de digitalisering van de IHM?
3. Hoe wordt de IHM digitaal beheerd in een veilige omgeving?
4. Hoe wordt de IHM gekoppeld aan een schip?
5. Hoe wordt er een simpele gebruikersomgeving rondom de digitale omgeving gemaakt?

3 Theoretisch kader

Binnen het theoretisch kader worden de onderzoeks vragen en kernbegrippen onderbouwd aan de hand van de theorie. Voordat de resultaten van de onderzoeks vragen worden voorgelegd zal er eerst wat verdieping worden gedaan met betrekking tot de kernbegrippen:

3.1 Definitie IHM

In de inleiding is de IHM besproken. Dit document is niet alleen een opsomming van gevaarlijke materialen, maar ook informatie over hun locatie en hoeveelheid. Deze inventarisatie omvat diverse soorten stoffen, zowel in vloeibare als vaste vorm, die bijzondere aandacht vereisen vanwege hun potentieel gevaarlijke aard. Voorbeelden van deze stoffen zijn asbest, kwikhoudend slib en verschillende soorten coatings die schadelijk kunnen zijn voor mens en milieu. In de tabel staan alle gevaarlijke stoffen die gedocumenteerd moeten worden in de IHM volgens de EU SSR regelgeving, zie Figuur 10.

Voor nieuwgebouwde schepen wordt er ook een IHM meegegeven door de scheepswerf. Dit is IHM part I, deze zal gedurende de levensduur moeten worden bijgehouden met alle structurele veranderingen op het schip. Part I vermeldt alle machines, uitrusting, materialen en coatings aan boord die als vaste onderdelen zijn geïnstalleerd. Vast betekent de omstandigheden waaronder uitrusting of materialen veilig aan het schip zijn bevestigd, bijvoorbeeld door lassen, bouten of gecementeerd. Ook zal er elke 5 jaar een routine check plaatsvinden die checkt of de informatie in de IHM part I correct is.

Aan het eind van de levensduur, wanneer het schip gerecycled wordt, zal er een part II 'Operationally generated wastes' en part III 'Stores' aan de IHM worden toegevoegd [5], zie figuur: 11 Het doel van Part II is om een overzicht te bieden van potentieel gevaarlijke afvalproducten die tijdens de normale bedrijfsvoering van het schip ontstaan. Dit zijn oliehoudende filters en slib, brandstof- en oliecontainers die niet volledig geleegd kunnen worden en asbesthoudende materialen die tijdens reparaties of onderhoudswerkzaamheden ontstaan. En Part III gaat over alle los gemonteerde uitrusting, zoals brandblussers, nood fakkels en reddingsboeien. Deze niet vast gemonteerde uitrusting die wel aan boord blijft wanneer het schip wordt gerecycled, moet worden vermeld in IHM Deel III.

3.2 Definitie digitalisering en verbetering

Een van de onderzoeks vragen stelt:

"Wat zijn de verbeterpunten die alleen door digitalisering de IHM waarborging verbeteren? "

Wat wordt er bedoeld met digitalisering? Digitalisering is het proces waarbij informatie wordt omgezet in een digitaal (oftewel een computer leesbaar) formaat. Het huidige IHM wordt vaak al digitaal gemaakt via een teksteditor, maar hier ligt de nadruk op het digitaal waarborgen van de IHM. Zo zou het nu vaak een document van papier op het schip zijn. Het digitaal waarborgen kan vele vormen aannemen zolang het maar binnen een computer zit. En met waarborgen wordt bedoeld het veilig stellen van de IHM zodat deze niet vervalt kan worden en alleen de desbetreffende stakeholders erbij kunnen.

3.3 Beïnvloeding stakeholders

Bij de waarborging van de IHM komen meerdere stakeholders kijken, en in het vraagstuk: 'Hoe worden verschillende stakeholders beïnvloed door de digitalisering van de IHM?' wordt er gekeken welke stakeholders hier mee te maken gaan krijgen. Hieronder staan de belangrijkste stakeholders en de functies die hierbij horen:

1. **Scheepseigenaar**, "De term 'scheepseigenaar' verwijst naar een individu of een bedrijfsentiteit die een schip bezit of leest. Deze entiteit is belast met het inhuren van de kapitein en de bemanning." [4]
2. **Rederij**, "Een rederij is een bedrijf dat zich bezighoudt met het exploiteren van schepen. Een rederij kan zich richten op verschillende soorten schepen, zoals vrachtschepen, tankers, cruiseschepen, vissersschepen, sleepboten en binnenvaartschepen. De taken van een rederij kunnen onder meer het beheer van de schepen, het plannen van routes, de bemanning, de lading en de bevoorrading omvatten." [11]
3. **Scheepsbouwer**, "Een scheepsbouwer is een ondernemer die verantwoordelijk is voor het ontwerpen en/of bouwen van schepen. Scheepsbouwers spelen een cruciale rol bij het creëren van veilige en betrouwbare schepen die geschikt zijn voor diverse maritieme toepassingen." [20]
4. **Hazmat bedrijf**, "Hazmat-veiligheid, een afkorting voor veiligheid van gevaarlijke materialen, heeft alles te maken met het zorgvuldig omgaan met potentieel risicovolle stoffen. Om een Hazmat-expert te worden moet een diepgaande training worden afgelegd, waarbij niet alleen de basisbeginselen van het omgaan met Hazmat worden behandeld, maar ook specifieke nuances met betrekking tot verschillende materialen." [17] Een hazmat bedrijf biedt verschillende hazmat experts die monsters kunnen afnemen op een schip om zo gevaarlijke stoffen te kunnen identificeren.
5. **Leverancier**, "Een leverancier is iemand die goederen of diensten levert tegen betaling. Een leverancier van een bedrijf of detailhandel kan een groothandel of een fabrikant zijn." [14]
6. **Havenautoriteiten**, "Havenautoriteiten zijn betrokken bij havenbeheer en de promotie van de haven die zij beheren." [22]
7. **Scheepsrecyclingfaciliteiten**, "Een scheepsrecyclingfaciliteit is een gedefinieerd gebied dat een locatie, werf of faciliteit is die wordt gebruikt voor het recyclen van schepen en voldoet aan de vereisten die kunnen worden gespecificeerd door de regelgeving." [16]
8. **Classificatiemaatschappijen**, "Een classificatiemaatschappij of classificatieorganisatie is een niet-gouvernementele organisatie die technische normen vaststelt en handhaaft voor de bouw en exploitatie van schepen en offshore-structuren. Classificatiemaatschappijen certificeren dat de constructie van een vaartuig voldoet aan relevante normen en voeren regelmatig inspecties uit in dienst om voortdurende naleving van de normen te waarborgen." [13]

3.4 Begrippen voor het digitaal beheren van data

In het vraagstuk: "Hoe wordt de IHM beheerd in een digitale omgeving", wordt er dieper ingegaan op de digitale mogelijkheden voor het opslaan en beheren van de IHM. Het begrip 'digitaal' wordt hier gebruikt om aan te geven dat de gegevens veilig op een computer worden opgeslagen in de vorm van bytes. Dit betekent dat de informatie niet fysiek aanwezig is, maar in plaats daarvan wordt bewaard

op digitale media, wat diverse voordelen biedt zoals efficiëntie, toegankelijkheid en beveiliging. Er zijn vele geavanceerde technieken beschikbaar om digitale bestanden te beheren en op te slaan, elk met hun eigen specifieke voor- en nadelen. Denk bijvoorbeeld aan het gebruik van databases, cloudservers en blockchaintechnologie. De termen die tijdens dit onderzoek naar voren komen, worden hieronder uitgebreider toegelicht om de verschillende aspecten en mogelijkheden van digitale IHM-beheer beter te kunnen begrijpen.

1. **Database**, Een database is informatie die is opgezet voor eenvoudige toegang, beheer en bijwerking. Computerdatabases slaan typisch aggregaties van gegevensrecords of bestanden op die informatie bevatten, zoals verkooptransacties, klantgegevens, financiële gegevens en productinformatie" [18]
2. **Blockchain**, "Een blockchain is een gedistribueerde database of grootboek gedeeld tussen de knooppunten van een computernetwerk. Ze zijn het meest bekend vanwege hun cruciale rol in cryptocurrency-systemen voor het bikhouden van een veilige en gedecentraliseerde registratie van transacties, maar ze zijn niet beperkt tot cryptocurrency-gebruik. Blockchains kunnen worden gebruikt om gegevens in elke branche onveranderlijk te maken - de term die wordt gebruikt om de onmogelijkheid van wijziging te beschrijven." [10]
3. **Proof of Work**, "Proof of Work (PoW) beschrijft een consensusmechanisme dat een aanzienlijke hoeveelheid rekenkracht vereist van een netwerk van apparaten." [21]
4. **Cloud servers**, "Een cloudserver is een gepoolde, gecentraliseerde serverbron die wordt gehost en geleverd via een netwerk - meestal het internet - en op verzoek toegankelijk is voor meerdere gebruikers. Cloudservers kunnen alle dezelfde functies vervullen als een traditionele fysieke server, door rekenkracht, opslag en toepassingen te leveren." [28]
5. **Github**, GitHub is een website en cloudbaseerde service die ontwikkelaars helpt bij het opslaan en beheren van hun code, evenals bij het bikhouden en beheren van wijzigingen in hun code. [15]
6. **Mining**, Mining is het process wat wordt gebruikt voor het valideren van een blockchain transactie. Hiervoor wordt een consensus mechanisme gebruikt zoals Proof of Work. [3]
7. **Hash**, Een hash is een digitale vingerafdruk van een bestand. Wanneer data naar een hash wordt omgezet zal het een gecodeerde text zijn van een vaste lengte. Deze is uniek voor deze data, daarom kun je het een digitale vingerafdruk noemen. Deze kan je niet oplossen om de oorspronkelijke data terug te vinden. [25]

3.5 Begrippen voor de implementatie van de schip module

Bij het vraagstuk: "Hoe wordt de IHM gekoppeld aan een schip?" moet de term gekoppeld wat verder worden uitgelegd. Met koppelen wordt de literaire definitie 'met elkaar verbinden' bedoeld. En verbinden is het juiste woord hier, want er moet op het schip verbinding kunnen worden gemaakt met de server. De IHM wordt veilig opgeslagen op de server. Zie de server als een kluis. Op het schip moet een module worden geplaatst die kan zien wat voor documenten er in de kluis zitten, zonder de inhoud van die documenten te kunnen bekijken. Zo kan je zien wie er het laatst iets in heeft gedaan, en waarom het erin is gedaan. Deze module focust dus op de inhoud en het versiebeheer, en dit moet via een protocol data kunnen ontvangen en sturen naar de server. In het onderzoek wordt gekeken naar verschillende manieren voor de gebruiker om toegang te krijgen tot deze module en hoe de module verbinding maakt met de server. Hierbij komen de volgende termen aan bod:

1. **NFC**, "NFC, wat staat voor near-field communication, is een technologie waarmee apparaten zoals telefoons en smartwatches kleine stukjes gegevens kunnen uitwisselen met andere apparaten en NFC-uitgeruste kaarten kunnen lezen over relatief korte afstanden." [12]
2. **RFID**, "Radio Frequency Identification (RFID) is een technologie die radiofrequenties gebruikt om passief een getagd object te identificeren. Het wordt gebruikt in verschillende commerciële en industriële toepassingen, van het volgen van items langs een toeleveringsketen tot het bijhouden van uitgeleende items in een bibliotheek." [9]
3. **Biometrische sensoren**, "Een biometrisch apparaat is gebaseerd op een technologie die een persoon kan identificeren aan de hand van hun unieke gezichtskenmerken, vingerafdrukken, handtekeningen, DNA of irismotief." [23]
4. **Bluetooth**, "Bluetooth is een draadloze communicatietechnologie op korte afstand die apparaten zoals mobiele telefoons, computers en randapparatuur in staat stelt om gegevens of spraak draadloos over een korte afstand te verzenden." [27]
5. **LoRa(WAN)**, LoRa is een draadloze modulatietechniek afgeleid van Chirp Spread Spectrum (CSS) technologie. Het codeert informatie op radiogolven met behulp van chirp pulsen, vergelijkbaar met de manier waarop dolfijnen en vleermuizen communiceren! LoRa-gemoduleerde transmissie is robuust tegen storingen en kan over grote afstanden worden ontvangen.
LoRaWAN is een Media Access Control (MAC) laagprotocol gebouwd bovenop LoRa-modulatie. Het is een softwarelaag die definiert hoe apparaten de LoRa-hardware gebruiken, bijvoorbeeld wanneer ze verzenden, en het formaat van berichten. Hiermee kan er een LoRaWAN-netwerkserver worden opgezet die kan communiceren met alle LoRa apparaten binnen bereik.[26]
6. **TTN**, The Things Network is een wereldwijd samenwerkend Internet of Things-ecosysteem dat netwerken, apparaten en oplossingen creëert met behulp van LoRaWAN [1]
7. **EEPROM**, (electrically erasable programmable read-only memory), is een stuk computer geheugen dat het mogelijk maakt dat individuele bytes gegevens gewist en opnieuw geprogrammeerd kunnen worden. EEPROM wordt meestal gebruikt om kleine hoeveelheden gegevens op te slaan in computers en andere elektronische apparaten. [2]

4 Methodologie

In deze scriptie over de naleving van de certificering van de IHM op schepen verbeteren met behulp van digitalisering, wordt er gebruik gemaakt van literatuur onderzoeken. Er worden twee literatuuronderzoeken uitgevoerd voor twee van de meest belangrijke deelvragen. In het onderzoek: "Hoe wordt de IHM digitaal beheerd in een veilige omgeving?" wordt er gekeken naar de digitale methodes die kunnen worden gebruikt voor het opslaan van de IHM. In het onderzoek: "Hoe wordt de IHM aan een schip gekoppeld" wordt er gekeken naar de module die op het schip zou worden geplaatst, inclusief een authenticatie proces en hoe deze kan verbinden met de digitale server waar de IHM staat opgeslagen.

De literatuuronderzoeken zijn gericht op het verzamelen en analyseren van online artikelen die onze vraagstukken kunnen beantwoorden. Voor het digitaliseren van de IHM zijn er nog geen papers of andere artikels over dit onderwerp. De conclusie moet dus voortkomen uit de literatuur onderzoeken. In de technische sector worden vaak technische vragen beantwoord in online artikels, gepubliceerd op hun eigen website. Hier kan je gemakkelijk definities en uitleg vinden over alle vraagstukken die worden gesteld in ons onderzoek. Vaak zijn er meerder artikels die dezelfde vraag beantwoorden en zo kan er makkelijk gekeken worden of de informatie kloppend is door deze met elkaar te vergelijken. Bij de literatuuronderzoeken zijn vrijwel alle bronnen online artikels.

Ook wordt er een simpele case study gebruikt van DNV's IHM manager. Simpel omdat deze analyse is gebaseerd op de verkoop pagina waar de features worden uitgelegd. Dit product is niet aangeschaft voor een uitgebreide case study. Op de website bevindt zich een video, een overview en meerder afbeeldingen. Al deze informatie is ge-analyseerde om zo de features van dat systeem na te lopen en te vergelijken met het systeem dat in dit onderzoek wordt voorgedragen.

Tot slot wordt er met een experimentele testen gekeken wat de maximale capaciteiten van het systeem zijn. Testen zijn afgelegd in het testplan. En andere resultaten worden verder uitgelegd in de scriptie. In dit testplan worden eerst de individuele functies getest van het product. In deze testen worden ook 'edge cases' meegenomen. Edge cases zijn scenario's waar je probeert het systeem te breken, door dingen te proberen waar het systeem niet voor bedoeld is. Nadat de testen voor de individuele functies inclusief edge cases zijn uitgevoerd is er een laatste test die de gehele werking van het systeem probeert te demonstreren. Deze test bevat alle vorige testen achtereenvolgend om te kijken of de continuïteit en samenwerking van de features goed werkt. De testen zijn ook ontwikkeld om de vereiste doelen van de scope te demonstreren. Als alle testen succesvol zijn, wordt de werking van het systeem bewezen.

5 Resultaten

5.1 Wat zijn de verbeterpunten die alleen door digitalisering de IHM waarborging verbeteren?

Door het huidige IHM proces te analyseren en te spreken met een expert (de product owner) kunnen de huidige problemen in het IHM-proces worden gedefinieerd. Door eerst naar de huidige problemen te kijken kunnen hiervoor oplossingen worden bedacht. Deze oplossingen worden gebruikt om zo de systeem vereisten op te stellen.

Huidige problem:

1. **Betrouwbaarheid informatie**, het belangrijkste verbeterpunt is de betrouwbaarheid van het document. Op de huidige manier heeft de IHM geen manier om te weten of de informatie kloppend is of vervalst. Dit document wordt als PDF aangeleverd maar met een simpele conversie kan je deze aanpassen in een tekst editor.
2. **Versiebeheer**, de IHM heeft vaak geen versiebeheer. Dit is erg onhandig al helemaal omdat dit document van eigenaar kan veranderen. Dan is het onmogelijk om goed terug te zien wie wat heeft gedaan. Vaak zullen er wel datums en certificaten instaan, maar zoals het vorig punt stelt: dit is makkelijk te vervalsen.
3. **Behouden document**, een digitaal document moet ergens veilig worden opgeslagen. Aangezien het beheren wordt overgelaten aan de schip owner kan dit fout gaan. Ookal wordt dit document uitgeprint moet het voor vele jaren ergens veilig worden opgeslagen met backups.
4. **Toegang document**, als stakeholders de IHM willen inzien moet de PDF worden doorgestuurd of ze moeten langskomen op het schip om de uitgeprinte versie door te lezen. Dit is allebei onhandig voor de stakeholders

Oplossingen:

1. **Betrouwbaarheid informatie**, Om de betrouwbaarheid te verbeteren moet de IHM na goedkeuring niet meer aanpasbaar zijn. Via een digitaal systeem kan je toegang verlenen om een bestand te bekijken maar aanpassingen onmogelijk zijn.
2. **Versiebeheer**, met een digitaal systeem kan je makkelijker loggen wie aanpassingen heeft gedaan, wanneer dit is gebeurd en wat de aanpassing was.
3. **Behouden document**, door dit document op een server op te slaan is het makkelijker te behouden. Ook kan je een backup server gebruiken voor extra veiligheid.
4. **Toegang document**, met een digitaal systeem kun je accounts gebruiken voor de verschillende stakeholders en ze bepaalde rechten geven. Dan kunnen ze vanaf werk of thuis digitaal veilig inloggen. Om de IHM aan boord van het schip te bekijken zal een module kunnen worden geïnstalleerd die verbinding maakt met het server om zo de IHM informatie te kunnen bekijken.

Systeem vereisten:

Met de voortgekomen oplossingen voor de huidige problemen ontstaat er al een idee voor het systeem. Zo is de betrouwbaarheid het belangrijkste. Met de nadruk liggende op on-aanpasbaarheid van de IHM na goedkeuring. Wanneer de IHM is geüpload naar het systeem zal deze niet aanpasbaar zijn. Versiebeheer is ook erg belangrijk en zo zullen alle vorige versies van de IHM ook nog zichtbaar moeten zijn. Bij elke versie zal relevante informatie zoals het tijdstip en de persoon of het bedrijf dat verantwoordelijk was voor de verandering. Om de stakeholders makkelijk toe te laten zal er een webserver kunnen worden gebruikt waarvoor je een account nodig hebt om in te loggen. Hierop zijn verschillende accounts voor de verschillende rollen die de stakeholders uitvoeren. Tot slot is het vereist voor de IHM om nog gelinkt te zijn aan een schip. Hiervoor zal een module op het schip worden geïnstalleerd dat kan verbinden met het server om zo informatie te laten zien.

In tabel 1, zijn de vereiste van het concept uitgeschreven met de criteria die bij elke vereist hoort.

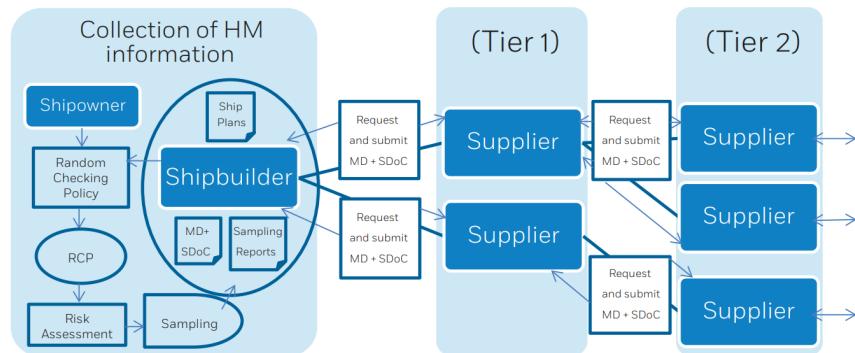
ID	Vereiste	Criteria
1	In de webinterface kunnen geen bestanden worden aangepast, alleen uitgelezen.	1. De webinterface biedt alleen mogelijkheid tot downloaden van geüploade bestanden.
2	Er wordt herhaaldelijk gekeken of alle bestanden nog onveranderd zijn.	1. Er wordt herhaaldelijk een hash-check uitgevoerd op alle bestanden om te controleren of ze ongewijzigd zijn gebleven. 2. Als een wijziging wordt gedetecteerd, wordt dit onmiddellijk gelogd in de webinterface.
3	Nieuwere bestanden moeten door een account met de juiste rechten kunnen worden geüpload zonder de vorige versie te overschrijven. Ook worden gegevens gelogd zoals de datum, tijd en persoon.	1. Alleen geautoriseerde gebruikers met specifieke rechten kunnen nieuwe bestanden uploaden. 2. Elke upload resulteert in een nieuwe versie van het bestand, waarbij eerdere versies behouden blijven en toegankelijk zijn voor terugval. 3. Bij elke upload worden de datum, tijd en de identiteit van de uploader automatisch geregistreerd en gelogd.
4	Nieuwe versies van de IHM moeten eerst door een andere stakeholder worden goedgekeurd voordat deze definitief wordt geüpload op de server.	1. De aangewezen stakeholder moet goedkeuring geven voordat de nieuwe versie op de server wordt geüpload. 2. De webinterface laat zien welke versie nog moet worden goedgekeurd aan de relevante gebruikers.
5	De schipmodule moet altijd het versiebeheer van de server laten zien op het schip.	1. De versiebeheerinformatie omvat alle relevante details, zoals versiegeschiedenis, datum, tijd en uploader van de bestanden. 2. Bij verlies van verbinding toont de schipmodule de laatst opgehaalde versiebeheerinformatie totdat de verbinding hersteld is.

Tabel 1: Tabel van systeem vereisten

5.2 Hoe worden verschillende stakeholders beïnvloed door de digitalisering van de IHM

Bij het beheren van de IHM zijn er meerdere stakeholders waar rekening mee gehouden moet worden. Denk aan stakeholders zoals de scheepswerven, scheepsbouwers, leveranciers, scheepseigenaren, classificatie maatschappijen, havenautoriteiten, hazmat bedrijven, scheepsrecyclingfaciliteiten, etc. Aangezien sommige stakeholders direct verantwoordelijk zijn voor het beheren van de IHM is het handig om te bepalen welke stakeholders worden betrokken bij het digitaliseren van de IHM.

Voor nieuwe schepen zal de IHM worden aangeleverd door de scheepsbouwer. "De scheepsbouwer is verantwoordelijk voor het naleven van de relevante internationale eisen bij het installeren van HM aan boord van nieuwe schepen. In dit opzicht moet de conformiteit van Part I van de IHM aan het ontwerp- en constructiestadium worden vastgesteld aan de hand van de Supplier's Declaration of Conformity (SDoC) en de bijbehorende Material Declarations (MD) die van leveranciers zijn verzameld. Daarom moet de informatie die door de leveranciers wordt verstrekt adequaat zijn en naar tevredenheid van de scheepsbouwer. MD en SDoC van leveranciers moeten worden opgevraagd en verzameld door de scheepsbouwer zoals beschreven in Figuur 1." [8]

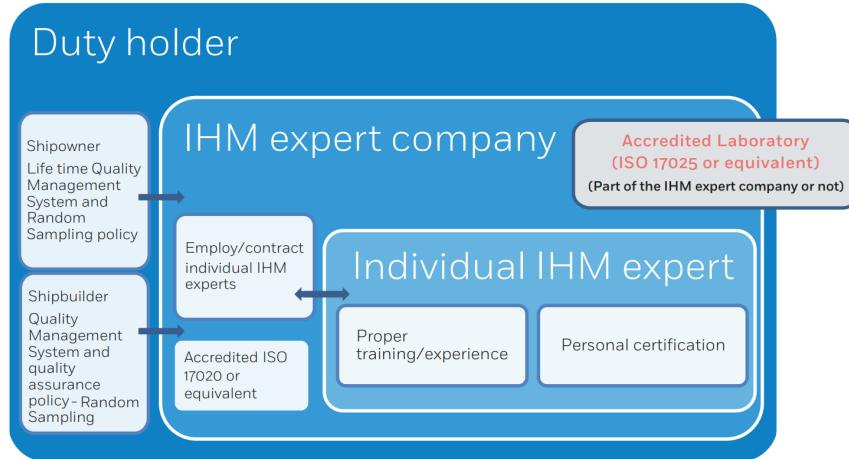


Figuur 1: Collection of HM information[8]

Soms zijn er meerdere lagen van leveranciers, die elkaar hun informatie aanbieden in de vormen van MD+SDoc. Deze worden door de schip builder gebruikt om een IHM aan te maken. "Echter, in de praktijk zijn er gevallen geweest waarbij willekeurige steekproeven hebben aangetoond dat MD's niet nauwkeurig waren." [8]. Omdat de informatie van de leveranciers niet altijd correct is moet de schip owner daarom ook een random checking policy gebruiken tijdens het bouwproces van het schip. Uiteindelijk is de schip builder verantwoordelijk voor de eerste versie van de IHM.

Voor bestaande schepen ziet het proces er als volgt uit Figuur 2. De 'duty holder' oftewel de scheepseigenaar of rederij zal verantwoordelijk zijn voor het aannemen van een expert hazmat bedrijf (vaak met een classificatie maatschappij als tussen link). Dit bedrijf stuurt een hazmat expert naar het schip toe die vervolgens monsters van het schip neemt om te bepalen welke gevaarlijke stoffen zich op het schip bevinden. Dit hazmat bedrijf zal de informatie doorgeven aan de classificatie maatschappij waar dit in

een IHM wordt gedocumenteerd. Elke 5 jaar wordt er een routine check uitgevoerd om zo de correctheid van de IHM bij te houden tijdens de levensduur.



Figuur 2: Optimum organisational framework[8]

"A software tool may be used to support the IHM development and maintenance process and the management of all the relevant documents, information and data." [8]. Het is toegestaan om een software tool of in dit geval een web interface te ontwikkelen om het IHM managen makkelijker te maken.

De samenwerking tussen al deze entiteiten over de hele levensduur van het IHM-proces vormt een aanzienlijke uitdaging. Maar met het voorgestelde systeem kan de samenwerking tussen de stakeholders aanzienlijk worden verbeterd met een gecentraliseerde webinterface waar de desbetreffende stakeholders toegang tot kunnen krijgen. Nu moet er gekeken worden welke stakeholders bepaalde rechten krijgen in het systeem. Denk aan accounts met verschillende rollen.

Classificatie maatschappijen zullen de meeste autoriteit hebben met betrekking tot de IHM, aangezien zij dienen als de belangrijkste regelgevende instanties. De rechten om te valideren wordt opzettelijk apart uiteengezet om te benadrukken dat alle updates moeten worden gevalideerd door de belanghebbenden die hiervoor verantwoordelijk zijn. Deze maatregel zorgt voor een transparant versiebeheer. Daarom zijn de Classificatie maatschappijen verantwoordelijk voor het goedkeuren van geüploade bestanden. Scheepsbouwers beheersen de levering van de IHM voor nieuw gebouwde schepen, terwijl hazmatbedrijven alleen verantwoordelijk zijn voor het afnemen van monsters en het verstrekken van resultaten aan de desbetreffende stakeholder. Scheepswerven en leveranciers kunnen nieuwe items leveren en deze aanpassingen aanbrengen in de IHM. Deze aanpassingen worden meegenomen in een nieuwe versie van de IHM omdat de vorige versie niet overschreden mag worden. Daarom krijgen ze recht voor het uploaden van bestanden. Voor alle andere belanghebbenden, zoals havenautoriteiten, scheepsrecyclingfaciliteiten en verzekeringsmaatschappijen, wordt alleen "bekijk" rechten gegeven, aangezien zij alleen als toezichthouder optreden. Dit kan geplot worden in een tabel als volgt:

Stakeholders	Recht bekijken	Recht uploaden	Recht goedkeuren
Classificatiemaatschappijen	+	X	+
Scheepseigenaar	+	+	X
Scheepsbouwer	+	+	X
Hazmat bedrijf	+	X	X
Leverancier	+	+	X
Havenautoriteiten	+	X	X
Scheepsrecyclingfaciliteiten	+	X	X

Tabel 2: Tabel van rechten binnen het systeem, + = wel recht, X = geen recht

5.3 Hoe wordt de IHM digitaal beheerd in een veilige omgeving??

Om te kijken welke digitalisering methods het beste gebruikt kunnen worden om de huidige problemen tijdens het beheren van de IHM op te lossen, wordt er onderzocht welke mogelijkheden er zijn voor het opslaan en beheren van digitale bestanden. Na verschillende methodes te vergelijken kan er een definitieve keuze worden gemaakt en daarmee wordt het prototype ontwikkelt.

In het onderzoek [6]: "Hoe wordt de IHM digitaal beheerd in een veilige omgeving?", is er onderzoek gedaan naar de mogelijkheden voor het opslaan van de IHM. Hierbij is er gekeken naar bestaande manieren voor data opslag(databases, cloud servers, blockchain, etc). Het gebruiken van een database [18] was overbodig. Databases zijn groot voor grotere aantallen data maar de IHM is maar één document waardoor het gebruiken van een database niet handig is. Het is mogelijk om de IHM op te slaan op een harde schijf die zich op het schip bevindt. Dit is simpel maar niet veilig. Omdat toegang verlenen alleen via het schip kan is deze oplossing ook onhandig voor de stakeholders. Wat handiger zou zijn is de IHM op een cloud server [28] opslaan. Hiermee kan je de stakeholders beter toegang geven. Zo kan altijd bij de IHM, waar je ook bent als je internetverbinding hebt. Hoewel het mogelijk is om ervoor te zorgen dat de IHM onveranderlijk is voor de stakeholders, de admin kan altijd nog aanpassingen maken. Een cloud platform zoals github [15] is gespecialiseerd in een uitgebreid versiebeheer. Dit wordt vaak gebruikt voor programmeer code maar kan ook documenten opslaan. Hoewel het versiebeheer uitstekend is en je altijd kunt zien wie de veranderingen maakt, is er nog steeds ruimte om de versiebeheer van de IHM aan te passen. Blockchain [10] is uitstekend voor onveranderlijkheid en transparantie. Een server die blockchain gebruikt zal een achtereenvolgende chain van blocks hebben die onaanpasbaar zijn. Dit is perfect voor de verschillende versies van de IHM. Zo kan er in elk block de volgende dingen opgeslagen worden:

- Data van de IHM opslaan
- Versiebeheer: De gebruiker die het heeft geupload en het tijdstip
- De vorige hash en huidige has om zo links te maken tussen de blocks. (Helpt met het valideren van de betrouwbaarheid chain)

'De conclusie uit het onderzoek [6] volg dus: "Uiteindelijk is GitHub goed voor robuust versiebeheer, gezamenlijk bewerken en gemakkelijke toegang. Terwijl blockchain goed is voor gegevensintegriteit, onveranderlijkheid en transparantie voor naleving van de regelgeving. Voor de use case is blockchain wat passender hoewel GitHub een redelijk alternatief is".

Na gekeken te hebben naar verschillende oplossingen is blockchain bovenop gekomen. Nu de techniek die gebruikt wordt om de IHM op te slaan vastgesteld is kan er een concept worden gemaakt. In het nieuwe concept zal de IHM geupload worden naar een block, deze is niet aanpasbaar. Als een block is

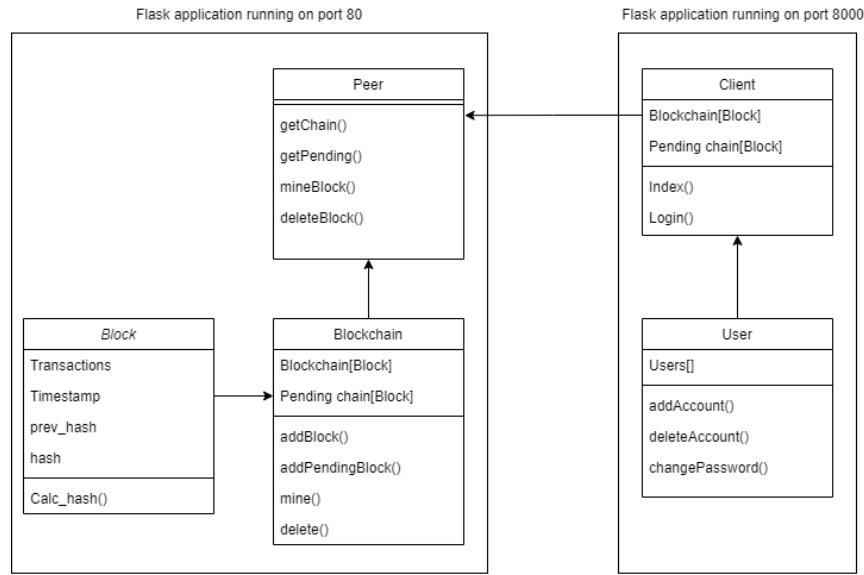
goedgekeurd door een consensus zal deze definitief in de chain worden gezet. Zo zijn vorige versies van de IHM ook nog zichtbaar als andere blocks. Bij elk block zal relevantie informatie zoals het tijdstip en de verantwoordelijke persoon te zien zijn. Nu het nieuwe concept is geschetst, wordt er gekeken naar bestaande markt oplossingen. Er waren nog weinig digitale IHM software dus er was maar een andere oplossing waar naar gekeken is. Dit was DNV's IHM manager. Deze biedt de volgende mogelijkheden:

1. De IHM van meerdere schepen beheren
2. Opslaan van Material Declaration (MD) en Suppliers' Declaration of Conformity (SDoC)
3. Wanneer er een aanpassing wordt gemaakt kan er een nieuwe versie worden gegenereerd.
4. Goed versiebeheer waar oude versies van de IHM niet worden verwijderd.
5. Een audit log waar alle aanpassingen te zien zijn en door welke gebruiker op welk tijdstip
6. Een gebruikersportaal waardoor derden ook toegang verleend kunnen krijgen.

Ons concept bevat al punten 4,5,6. En punten 1-3 vallen niet binnen de scope. De management tool gebruikt geen blockchain maar bestaat uit een database.

Er zijn een paar verschillende soorten blockchain netwerken: private, public en hybride[24]. Welke kunnen wij het best gebruiken? "Voor onze use-case is het beste om hybride of private blockchain te gebruiken. Een hybride netwerk is meer gedecentraliseerd en maakt het makkelijker om mensen toe te laten tot dit netwerk voor validaties, maar dit zorgt voor een complexere blockchain wat moeilijk valt te integreren. Terwijl de private blockchain efficiënter is met snellere transactie snelheden en lagere kosten. Ook is sensitieve informatie beter beschermd. Alleen is de private blockchain wel meer gecentraliseerd, wat een minder robuuste systeemarchitectuur is. En hoewel het netwerk schaalbaar is, is deze niet even goed schaalbaar als de hybride of public blockchain. Toch zal voor deze use-case een privé netwerk sneller en makkelijker zijn om te ontwikkelen, en biedt de juiste vereiste voor de opdrachtomschrijving" [6].

De IHM (een bestand van 10 Megabytes) is voor een block in de blockchain een groot bestand. In een block kan alleen de hash worden opgeslagen of ook de rauwe data (alle losse bytes) kan in een block worden gezet. "De veiligste manier is om een bestand volledig op te slaan in de blockchain. Dit betekent dat de data van het bestand in de blockchain wordt gezet. Om het bestand te bekijken moet je dan het bestand opnieuw bouwen met de data uit de blockchain en zo kan je het bestand bekijken. Op deze manier is het bijna onmogelijk om de IHM te aanpassen en frauderen" [6]. Tot slot moet er gekeken worden naar een consensus mechanisme voor blocks, zodat alleen betrouwbare blocks definitief op de chain worden gezet. "Als de informatie (van een block) volgens alle stakeholders correct is en dus goedgekeurd wordt zal het block definitief gechained worden aan het vorige block. Als een van de stakeholders dit niet goedkeurt zal het block niet worden gechained en moet er tussen de stakeholders overlegd worden over het probleem. Binnen het blockchain netwerk moet een rollensysteem worden gemaakt. Waar verschillende accounts andere rechten hebben (Alleen lezen, Alleen valideren, Alleen Uploaden)" [6]. De consensus is dus menselijk. Met het nieuwe concept kan er een simpel design worden gemaakt, zie Figuur: 3



Figuur 3: Class Diagram

Dit private blockchain systeem wat gebruikt gaat worden is geprogrammeerd in python. Classes zoals block en blockchain worden gebruikt om digitaal een blockchain systeem te simuleren. Voor de hashes[25] wordt gebruik gemaakt van Sha-256. Binnen de class blockchain bevinden zich twee lists, de gefinaliseerde blockchain en de 'pending' blockchain. Als consensus mechanisme wordt de feedback van de stakeholders gebruik die als goedkeuring het block 'minen'[3]. Dus voordat een block definitief wordt toegevoegd aan de blockchain zal deze worden opgeslagen in de pending list. Zodra het block wordt gemiced zal deze op de definitieve blockchain worden geplaatst. Voor het minen wordt een simpel Proof of Work[21] gebruikt. Hierbij wordt de nonce (Numbers Only Used Once) van het block iteratief aangepast totdat de hash van het block begint met x aantal nullen. Het aantal nullen is de moeilijkheidsgraad. Omdat de inhoud van een bestand best groot kan zijn en ook wordt gebruikt voor het hashen zal de moeilijkheidsgraad (aantal nullen) dus niet te hoog zijn want anders duurt het genereren van een hash erg lang.. Door de hash te beginnen met een aantal nullen kan er goed worden afgeleid of alle hashes in orde zijn. De blockchain en pending lists worden als JSON in een txt bestand opgeslagen binnen de server. Dus als de server opnieuw zou opstarten raakt de blockchain niet verloren. In elk block worden de volgende gegevens opgeslagen op de volgende manier:

1. **Transactions**, de velden die worden verkregen van de gebruiker en het bestand:
 - (a) **user**, de gebruiker die het bestand heeft geüpload
 - (b) **description**, beschrijving van de inhoud van het bestand
 - (c) **v_file**, de naam van het bestand
 - (d) **file_data**, inhoud van het bestand
 - (e) **file_size**, de grootte van het bestand
2. **Timestamp**, de tijd wanneer het block is gemaakt

3. **Prev_hash**, de hash van het vorige block in de chain
4. **Nonce**, getal wat wordt gebruikt voor PoW
5. **Hash**, de hash van dit block

Deze opstelling is voorgekomen uit de structuur vaak gebruik in bitcoin [19]. Met als toevoeging velden zoals: description, v_file, file_data en file_size.

Dit programma wordt uitgevoerd op een server. Met gebruik van flask wordt er een client en peer script uitgevoerd. Deze runnen op hetzelfde IP met andere ports. In de peer wordt de blockchain en alle andere relevante functies behandeld. In de client worden de IHM en de stakeholder accounts gemanaged, ook wordt de website presentatie hier gedaan. In de client is het mogelijk om: accounts te maken voor verschillende stakeholder rollen (admin, bekijker, uploader, validator), wachtwoord te veranderen van ingelogde account, de blockchain te bekijken, een bestand te uploaden naar de 'pending' blockchain, blocks in de pending blockchain goedkeuren of verwijderen en downloaden van bestanden op de pending en definitieve blockchain.

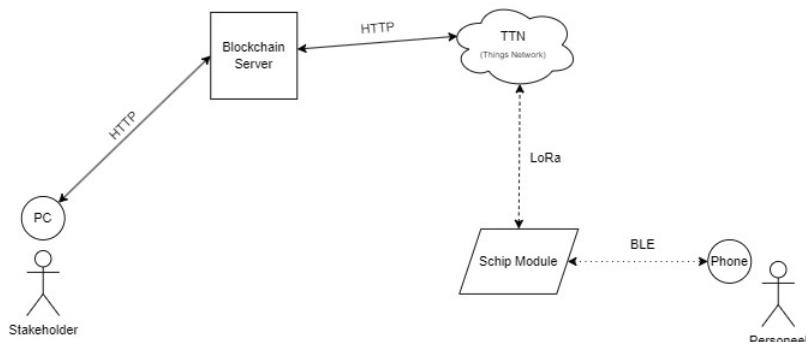
Om een officieel https certificaat te krijgen heb je eerst een domeinnaam nodig. Aangezien deze server nog wordt gebruikt als prototype is er geen domeinnaam geregistreerd. Wel kunnen er zelf gegenereerde SSL certificaten gebruikt worden voor een https connectie. Zo wordt de data die wordt verstuurd tussen de server en de gebruiker encrypted, en als deze onderschept worden door een hacker ze niet uit te lezen zijn. Omdat de SLL certificaten niet officieel gecertificeerd zijn geeft het browser een waarschuwing wanneer je de site bezoekt, dit probleem wordt automatisch verholpen in het gefinaliseerd product als er een domeinnaam is geregistreerd zodat de website dan een officieel SLL certificaat aanvragen.

5.4 Hoe wordt de IHM gekoppeld aan een schip?

Om de IHM te koppelen aan een schip wordt er een module geïnstalleerd op het schip wat verbinding kan maken met de server. Zo kan de aanwezigheid en het versiebeheer toch bekijken worden op het schip. Dit is een vereiste aangezien elk schip boven 500 Ton een IHM moet dragen. Zo wordt er gekeken naar verschillende toegang methodes voor de schip module en een communicatie methode voor de verbinding tussen de module en de server.

In het onderzoek: "Hoe wordt de IHM gekoppeld aan een schip?" [7], is er gekeken naar verschillende authenticatie methodes. In dit onderzoek was er vanuit gegaan dat de module beveiligd moest zijn. Later is vastgesteld met de opdrachtgever dat omdat de module alleen toegankelijk is op het schip zelf, de fysieke plek genoeg beveiliging is. Maar dit onderzoek heeft nogsteeds zijn waarde want hierdoor is wel een goede oplossing uit voorgekomen. Er is gekeken naar Smart cards, met NFC [12] en RFID [9] functionaliteit. Vanuit deze twee is NFC gekozen want deze is beter voor het versturen van informatie terwijl RFID beter is voor het nagaan van informatie zoals inventarisering. Smart cards zijn handig om fysieke toegang te verlenen maar aangezien het erg ingewikkeld is om de NFC-functionaliteit via een mobiele telefoon na te bootsen moeten er fysieke kaarten worden gebruikt. Dat betekent dat er iemand op het schip verantwoordelijk is voor het verlenen van toegang via deze kaarten die dan ook weer veilig moeten worden opgeborgen. Mogelijke oplossing, maar niet altijd even handig. Biometrische scanners [23] zoals een vingerafdruk zijn erg goed voor een systeem dat erg goed beveiligd moet worden maar voor deze use-case overbodig. Wachtwoorden gebruiken voor het authenticatie proces is dan ook overbodig aangezien deze module niet deze extra beveiligingslaag nodig heeft. Indien er toch gebruik gemaakt gaat worden van wachtwoorden zullen er ook nog extra maatregelen genomen kunnen worden, zoals

two-factor authentication en dagelijkse nieuwe wachtwoorden. Bluetooth was de gekozen oplossing uit het onderzoek omdat dit het handigste is voor toegang tot de module. Dit heeft voldoende beveiliging aangezien vrijwel iedereen op het schip gemachtigd is om dit document te bekijken en via Bluetooth met een maximale bereik van 10 meter [27] kan je dus alleen verbinden als je je op het schip bevindt. Ook is dit handig want er kan via een mobiele telefoon app data worden uitgelezen, dus een dan heeft de module niet groot scherm nodig. In het onderzoek[7] is er ook gekeken naar mogelijkheden om verbinding te maken met de blockchain server. Zo heb je satelliet verbinding, mobiele datanetwerken en LoRaWAN[26]. Naar Wifi is niet gekeken, aangezien deze module niet afhankelijk moet zijn van het schip's internetverbinding. Satelliet en mobiele datanetwerken bleken gelijk al duurder dan Lora(WAN), wel met veel hogere bandbreedte en snelheden. Maar aangezien een hele snelle verbinding niet de prioriteit is volgens de vereiste, komt LoRa(WAN) toch dichterbij de scope. Met LoRa's kleinere bandbreedte is het niet mogelijk om grote bestanden zoals de IHM te downloaden. Hoewel het fijn was geweest om hele bestanden te kunnen downloaden met deze module is dit vaak niet nodig. Wat belangrijker is dat de blockchain overzichtelijk weer te geven is. Dit is wel mogelijk via LoRa. Nu de communicatie manieren zijn vastgesteld kan de systeem architectuur worden weergegeven, zie Figuur 4:



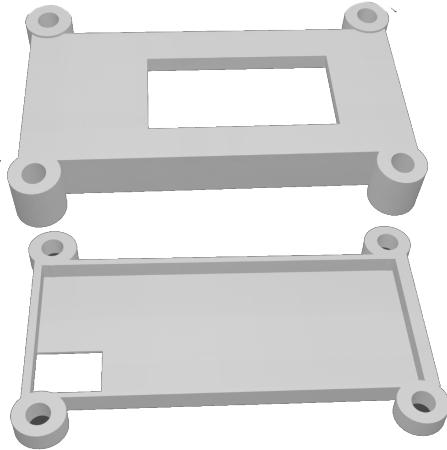
Figuur 4: Architectuur van dit systeem

Je ziet dat de blockchain server alleen via HTTP te bereiken is. Met de webinterface kunnen de stakeholders inloggen op de server om het systeem te beheren. De module op het schip kan bemachtigd worden via BLE (Bluetooth Low Energy) op een mobiele telefoon. Als de module merkt dat er een bluetooth verbinding ontstaat stuurt deze een LoRa signaal, die verbinding maakt met een LoRaWAN gateway in de buurt. Deze gateway is verbonden met TTN (The Things Network). Met TTN kan er een webrequest gemaakt worden naar de server om de blockchain informatie door te sturen, terug naar de schip module. En dan kan via een app op de telefoon deze informatie te zien zijn.

Nu vastgesteld is dat Bluetooth and LoRa worden gebruikt is het handig om de module compact te houden en een microcontroller aanschaffen die deze componenten ingebouwd heeft. Hierbij kwam je al snel bij ESP32S3 development boards. De Heltec Wi-Fi LoRa 32 was gekozen maar dankzij de lange levertijd is er overgestapt naar de Heltec Wireless Tracker 1.1. Dit is een nieuw model en heeft dezelfde ondersteuning voor LoRa en Bluetooth. De ontwikkeltijd voor dit product was vrij lang, aangezien bij het ontwikkelen meerdere obscure problemen kwamen kijken. Een flowchart en de uitleg hiervan is te vinden in de bijlage.

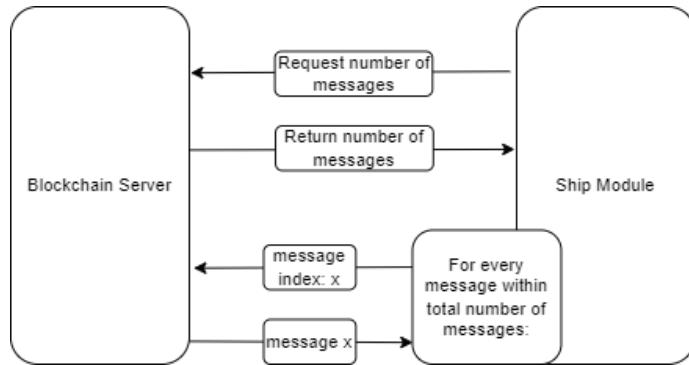
De behuizing voor de microcontroller moet strak en compact zijn. Daarom is ervoor gekozen om deze

te 3D-printen, wat het mogelijk maakt de behuizing precies op maat te maken en de juiste robuustheid te bieden voor het prototype. Voor de microcontroller is een behuizing ontworpen die er precies omheen past, met openingen voor het scherm, de USB-poort en de LoRa-antenneconnector (zie Figuur 5). Aan alle vier hoeken bevinden zich schroefgaten om de boven- en onderkant met elkaar te bevestigen. Met lange schroeven kan de behuizing ook aan de muur worden gemonteerd. In de bijlage zijn een render en een foto van de geprinte behuizing te vinden. 13, 12



Figuur 5: 3D ontwerp Bovenkant (boven) en Onderkant (onder) van behuizing

De twee problemen ontstonden tijdens het ontwikkelen. De antenne was niet goed genoeg om LoRa berichten terug te krijgen van de gateway. Hierdoor kon dus nooit een goede connectie worden opgezet met de LoraWAN gateway en dus TTN. Ook was de server van de hogeschool Rotterdam niet in staat om berichten te ontvangen van TTN, dit kwam omdat deze server alleen connecties binnen Nederland toe liet, en dit kon niet verandert worden. Zo is er dus een nieuwe antenne besteld, en de server is gemigreerd naar Microsoft Azure. De vereiste van de antenne is dat deze een SMA aansluiting heeft en een bereik rond de 868MHz. Microsoft Azure biedt mogelijkheden om virtual machines te hosten. Vanwege voorafgaande ervaring en de goedkope prijs is dit gekozen als nieuwe ontwikkelomgeving. Net als het vorige server van de Hogeschool Rotterdam is er gekozen voor de ubuntu omgeving. Hierop is de code van het blockchain server via github gemigreerd naar de virtual machine. Door opnieuw de benodigde libraries te downloaden en een port open te zetten voor de client werkte alles weer goed. Door nu een uplink message te sturen naar TTN wordt er automatisch een webrequest gemaakt naar de /webrequest pagina op het nieuwe IP. Door deze webpagina te bezoeken wordt de blockchain in bytes naar TTN gestuurd. Dit werkte goed, totdat de blockchain erg lang werd. TTN gaf aan dat de max bytes per message 242 is. Dat betekent dat de code omgeschreven moet worden om de blockchain in te delen in stukken van 242 bytes. Dat betekend dus dat er meerdere berichten naar TTN worden gestuurd. Dat betekende ook dat in de code voor de microcontroller deze meerdere berichten achtereenvolgend moet ontvangen en deze zelf weer achter elkaar plakken. Er moet dus zelf een protocol verzonden worden om de data goed over te sturen op een variabele manier om zo rekening te houden met de verschillende lengtes van de blockchain.



Figuur 6: Communicatie Protocol Blockchain server en schip module

In figuur 6 zie je het ontworpen protocol. De microcontroller stuurt een bericht naar de blockchain server waarmee deze vraagt hoeveel berichten er moeten worden gestuurd. De blockchain server antwoordt met het aantal berichten. De module ontvangt het totaal en start een lus die door elk bericht loopt. De huidige index van het bericht wordt doorgestuurd naar de blockchain server zodat deze weet welk bericht deze moet ophalen en als dit bericht verloren gaat stuurt de microcontroller hetzelfde nummer nog een keer om zo het juiste bericht op te halen.

Na wat testen bleek dat meerdere pakketten sturen van 242 bytes niet goed werkte op de microcontroller en dat met een grootte van 100 of 80 bytes het langzamer maar wel beter werkte. Zo waren alle berichten compleet, leesbaar en crashte de microcontroller niet (dit gebeurde bij lange berichten soms).

De taak van het bluetooth component is erg simpel. Wacht totdat een telefoon een verbinding aanmaakt. Stuur via LoRa een message naar de blockchain server en krijg als antwoord de blockchain in string vorm terug. Deze kan dan via bluetooth verstuurd worden naar de telefoon om uitgelezen te worden. De microcontroller gebruikt BLE (Bluetooth Low Energy). Het verbinden via bluetooth was erg makkelijk. Via de gratis app nRF connect kan je erg makkelijk verbinden met de ESP32 en de data ontvangen die wordt doorgestuurd. Het probleem komt pas wanneer je een string wilt sturen. Deze app leest alleen de bytes uit dus tekst is niet zichtbaar. Er moet dus een simpele app ontwikkeld worden die de bytes omzet naar tekst en dit leesbaar weergeeft. Met MIT app inventor is er snel een prototype gemaakt. Deze app kan met de ESP32 verbinden en data ontvangen. Het zet de data om naar tekst. Dit werkte tot 20 karakters. Omdat BLE niet meer dan 20 bytes kan versturen moet de code dus worden aangepast. Zo deelt de microcontroller eerst de tekst in stukken van 20. Iteratief worden er steeds 20 karakters verstuurd in pakketjes en in de app worden deze aan elkaar geplakt zodat je uiteindelijk de hele blockchain regel te zien krijgt. Dit gaat nogsteeds erg snel met ongeveer 5 ms per bericht. Dus zelfs al heb je een een blockchain van 1000 bytes (1000 letters) zal je binnen ongeveer 0.2 seconde dit kunnen uitlezen (pas nadat alle LoRa berichten zijn opgehaald en dat duurt wel wat langer).

Omdat de schipmodule zich ook op plekken gaat bevinden waar er geen LoRaWAN bereik is moet de laatste blockchain data worden opgeslagen. Zo kan er zonder een connectie met de server het laatste opgehaalde bericht nogsteeds weergegeven worden in de app. EEPROM [2] wordt gebruikt om deze data op te slaan in het interne geheugen. Als de module opnieuw wordt gestart blijft deze informatie opgeslagen. Maar de ESP32 die wordt gebruikt voor dit project heeft geen EEPROM. Wel heeft het flash

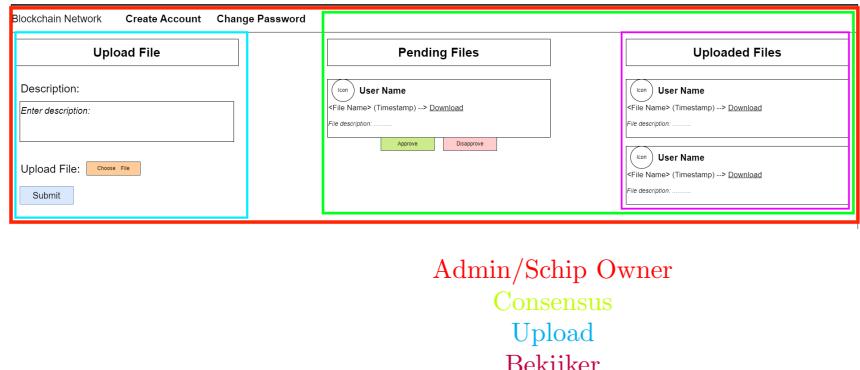
geheugen, wat is gebaseerd op EEPROM technologie. Zo gebruikt de code ook de Arduino EEPROM.h library die al functies bevat zoals EEPROM.read, en EEPROM.write. Deze library emuleert de functionaliteit van de EEPROM door gegevens naar/van het FLASH-geheugen te schrijven en te lezen. Deze implementatie is gebaseerd op de ESP32 NVS (Non-Volatile Storage) drivercode. In de geheugen map van het flash geheugen is de non-volatile storage 0x5000 oftewel 20480 bytes oftewel 20kB. Dit zal meer dan genoeg zijn om een langere blockchain als bytes op te slaan. Hoewel deze methode onafhankelijk werkte, na het combineren met de LoRa en BLE code zorgde het opslaan en uitlezen van bestanden voor het crashen van de microcontroller. Een andere methode met gebruik van de Little FileSystem library had hetzelfde probleem. Enkele oorzaken kunnen zijn: geheugen belasting van de RAM doordat de LoRa en BLE implementaties veel geheugen gebruiken, de interrupts van LoRaWAN en/of BLE kunnen interfereren met de timing van bestandsbewerkingen of de stack van bepaalde taken loopt vol door de complexiteit de code. Helaas was er niet genoeg tijd om dit probleem op te lossen. De EEPROM en LittleFS code is allebij standalone getest en dit werkte. Misschien op een andere microcontroller met meer geheugen zou dit probleem zich niet optreden. Voorlopig staat de laatste opgehaalde blockchain opgeslagen als variabele in de code, deze wordt ingevuld als er een keer succesvol verbinding is gemaakt.

Aangezien LoRaWAN bereik op sommige plekken nog niet aanwezig is, kan de module ook wifi gebruiken. De module kan in principe volledige zelfstandig werken met LoRa, maar als het huidige schip ook een wifi netwerk heeft kan deze ook gebruikt worden om verbinding te maken met het blockchain server. Om dit te realiseren zijn er in de app twee nieuwe velden toegevoegd waar de naam van het wifi netwerk en het wachtwoord kunnen worden ingevoerd. Eenmaal ingevuld en verzonden kan de microcontroller met de ESP32 chip verbinding maken met het wifi netwerk. Toen de wifi code werd toegevoegd aan de code van de schip module ontstond er een probleem. De code en de geïmplementeerde libraries waren te groot geworden om te uploaden. Na onnodige code verwijderd te hebben en een poging tot het omschrijven van de RadioLib library was de code nogsteeds te groot. Daarom is een aparte code geschreven die in plaats van een LoRa verbinding maakt, een wifi verbinding maakt. Zo kan de werking van de schip module ook worden aangetoond in een gebied zonder LoRa bereik. Om dit te doen moet er van te voren de wifi versie van de code naar de microcontroller worden geüpload. In het uiteindelijke product zou het ideaal zijn om beide communicatie methodes te kunnen gebruiken. Maar daarvoor moeten de twee codes worden samengebracht zonder te groot te worden voor het geheugen van de microcontroller. Of in het uiteindelijke product kan een andere microcontroller gebruikt worden met meer geheugen.

5.5 Hoe wordt een simpele gebruikersomgeving rondom de digitale omgeving gemaakt?

Aangezien de module en de webinterface gaan worden gebruikt door niet-technisch personeel is het belangrijk om de website en app erg gebruiksvriendelijk te maken. Dit systeem moet voor de gebruiker fijn zijn om te gebruiken en makkelijk om te begrijpen. Een belangrijk punt voor de webinterface is dat deze modular moet zijn. Zo kunnen bepaalde accounts verschillende dingen zien. De bekijker mag bijvoorbeeld niet de 'pending' blockchain zien of toegang hebben tot de upload knop. Daarom moeten de upload, pending blockchain en definitieve blockchain aparte secties zijn die in de HTML makkelijk kunnen worden omgewisseld. Alleen de admin kan de gehele webinterface zien en kan nieuwe accounts toevoegen. Voor de website zijn er een paar schetsen gemaakt voor de admin omgeving. deze zijn te vinden in de bijlage: Figuur 14. Figuur 15. Figuur 16. Hoewel het ontwerp van 16 goed de blockchain laat zien, is het onhandig. Door de blocks van links naar rechts te laten gaan, zorg je dat de tekst ruimte

maar een kleine horizontale lengte heeft wat niet lekker leest als een block een lange beschrijving heeft. Ontwerpen 14 en 15 zijn allebei wat beter leesbaar. Om de modulariteit van dit ontwerp aan te tonen is 16 gebruikt. In het volgende figuur 7 zijn de verschillende modules omcirkeld met het account dat deze kan bekijken.

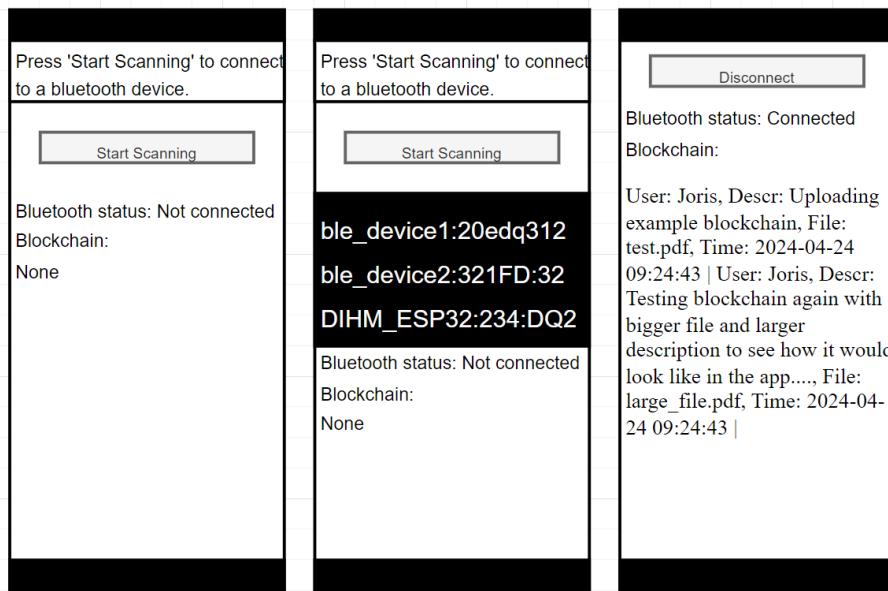


Figuur 7:

In de html code hebben de verschillende accounts allemaal hun eigen webpagina waar ze alleen recht hebben om de module te zien die hierboven zijn uitgelicht. Elk account heeft een rol, en deze wordt gebruikt om na het inloggen naar de juiste webpagina doorverwezen te worden. Het zal ook niet mogelijk zijn om naar een andere webpagina te gaan en daar de andere modules te bekijken want dan wordt het account gelijk terug gelinked naar zijn eigen webpagina. Hoewel de admin wel de pending list kan zien inclusief de knoppen voor het goedkeuren of afkeuren van een block zal alleen de consensus een block definitief op de blockchain kunnen zetten. Dit omdat anders de admin (waarschijnlijk de schip owner) zelf van alles kan goedkeuren wat niet de bedoeling is.

Nu de web interface behandelt is, kan de app behandelt worden. Deze app moet simpel zijn, met als enige taak: Verbinden met bluetooth en dan het weergeven van de blockchain. Het ontwerp zal dus de volgende functies moeten ondersteunen: scan voor bluetooth apparaten, verbind met bluetooth apparaat, en een plek om de blockchain weer te geven. Het volgende ontwerp is gemaakt 8: Wanneer de app wordt geopend leest de gebruiker gelijk de beknopte uitleg. Waarna de gebruiker op start scanning zal drukken. Er wordt een lijst gemaakt van alle bluetooth apparaten in de omgeving, maar de enigste waar verbonden mee kan worden is de DIHM-module. Eenmaal verbonden zal automatisch de blockchain worden opgehaald en laten zien in de app.

Vanwege wat problemen met LoRa (geen bereik, of slechte antenne) is er in de app een optie toegevoegd die werkt via WiFi. In de app kan je de naam en wachtwoord van een wifi netwerk invullen en zo zal deze module verbinding kunnen maken met het internet, dus in plaats van LoRa wordt hier via WiFi verbonden met de blockchain server. Als de wifi netwerk gegevens goed ingevuld zijn zal de huidige blockchain worden uitgelezen in de app. In de code van de microcontroller probeerde ik de wifi en LoRa code in dezelfde code te implementeren, maar omdat deze samen veel libraries importeren werd de code te groot om te uploaden op de microcontroller. De huidige microcontroller's flash memory is niet groot genoeg om deze code te ondersteunen. Hoewel het misschien mogelijk is om de libraries en de code zo om te schrijven zodat de bestandsgrootte kleiner is, valt dit niet binnen de scope. De WiFi functionaliteit is volledig optioneel want de module kan ook zelfstandig met LoRa werken.



Figuur 8: Van links naar rechts. 1: Opening Pagina, 2: Na klik op Start Scanning, 3: Verbonden met bluetooth

6 Conclusie

Nu de resultaten besproken zijn is er genoeg informatie om de onderzoeks vragen te beantwoorden.

6.1 Dit zijn de verbeterpunten die door digitalisering de IHM waarborging verbeteren.

De huidige problemen met de IHM zijn:

- Betrouwbaarheid van informatie: Het is vaak niet mogelijk om te kijken of de informatie kloppend is.
- Versiebeheer: Er is geen goede manier om bij te houden wie wat heeft veranderd in het document.
- Opslag van documenten: De documenten moeten veilig worden opgeslagen, maar het beheer ervan wordt vaak aan de schip eigenaar overgelaten.
- Toegang tot documenten: Het verkrijgen van toegang tot de IHM is soms onhandig voor de stakeholders.

Deze problemen kunnen op de volgende manieren worden opgelost. Zo kan de betrouwbaarheid verbeteren door de documenten na goedkeuring aanpasbaar te maken. Het versiebeheer wordt verbeterd door logboeken bij te houden van wijzigingen. De documenten worden veilig opgeslagen op een server. Stakeholders krijgen makkelijke toegang door een accounts management systeem. Tot slot zal er een module op het schip komen om verbinding te maken met de server waardoor ook op het schip het logboek te zien is.

Het belangrijkste punt is betrouwbaarheid, dus on-aanpasbaarheid na goedkeuring is essentieel. Versiebeheer is belangrijk, alle vorige versies moeten zichtbaar zijn met relevante informatie over wijzigingen. Webserver met accounts voor verschillende rollen van stakeholders zorgt voor makkelijker toegang verlenen. Een module op het schip zorgt voor verbinding met de server en toont IHM-informatie.

6.2 Zo worden verschillende stakeholders beïnvloed door de digitalisering van de IHM.

Door te kijken naar de verloop van het IHM proces voor nieuwe gemaakte schepen en bestaande schepen is op te merken dat de volgende stakeholder het meeste worden beïnvloed door het proces heen: Scheepsbouwers, leveranciers, scheepseigenaren, classificatie maatschappijen, havenautoriteiten en IHM-experts. De samenwerking tussen al deze entiteiten kan aanzienlijk worden verbeterd met een gecentraliseerde webinterface waar de desbetreffende stakeholders toegang tot kunnen krijgen. Stakeholders krijgen bepaalde rechten in het systeem. zoals bekijken, uploaden en goedkeuren. Classificatiemaatschappijen dienen als de belangrijkste regelgevende instanties en krijgen recht voor het bekijken en goedkeuren. De scheepseigenaar is verantwoordelijk voor het beheren en mag dus ook nieuwe versies van de IHM uploaden. Scheepsbouwers en leveranciers beheersen de levering van de IHM voor nieuw gebouwde schepen en krijgen ook recht tot uploaden. Voor alle andere belanghebbenden (hazmat bedrijf, havenautoriteit en verzekeringsmaatschappijen) worden alleen "bekijk" rechten gegeven, aangezien zij alleen als toezichthouder optreden.

6.3 Zo wordt de IHM digitaal beheerd in een veilige omgeving.

Er is gekozen naar manieren om de IHM veilig op te slaan. Blockchain bleek de beste manier voor onveranderlijkheid en transparantie, wat de belangrijkste eigenschappen waren voor het veilig opslaan van de IHM. Daarom is voor dit project is een blockchain netwerk ontwikkelt. Binnen elk block zal een document staan, zoals de IHM. Elk vervolgend block zal eraan gechained worden en de hashes gelinked. Zo krijg je een veilige systeemarchitectuur en automatisch onveranderlijk versiebeheer. Er wordt een menselijke consensus gebruikt waar de classificatiemaatschappij de inhoud van een block moet goedkeuren voordat deze definitief in de blockchain wordt gezet. Wanneer het block wordt goedgekeurd wordt een simpel PoW gebruikt om de hash wat moeilijker te maken voor extra veiligheid. Elk block bevat de volgende fields: Transactions (user, description, v_file, file_data, file_size), Timestamp, Prev_hash, Nonce, Hash. Dit is gebaseerd op de structuur vaak gebruikt in bitcoin. Ook heeft de webinterface de mogelijkheid om accounts te maken en verwijderen, waarbij de wachtwoorden verandert kunnen worden.

6.4 Zo wordt de IHM gekoppeld aan een schip.

Om de IHM aan een schip te koppelen wordt hiervoor een module ontworpen. Na opties afgewogen te hebben is bluetooth bovenop gekomen. Omdat het gebruik van bluetooth is inbegrepen op elke hedendaagse smartphone, zal er geen scherm nodig zijn om de blockchain op uit te lezen. Want dit kan nu via het scherm van de mobiele telefoon. Als de gebruiker zich binnen het bereik van de module bevindt 5-10m, kan de mobiele telefoon verbinden over bluetooth. De module maakt verbinding met de blockchain server via LoRa, dit is een draadloze modulatie techniek, die informatie via radio golven over grote afstanden stuurt (2-5 km). Als binnen dit bereik een publieke LoRaWAN gateway zit, kan deze verbinding maken met het internet. Realistisch gezien zal de module niet altijd verbinding nodig hebben als het laatste bericht nog wel opgeslagen staat op de microcontroller, want aanpassingen in de IHM gebeuren niet vaak (minstens elke 5 jaar). De microcontroller is de Heltec Wireless Tracker, want deze had ingebouwde bluetooth en Lora modules. Door in TTN een webhook aan te maken voor de blockchain server, zal na een succesvolle LoRa verbinding deze de tekst over LoRa terugsturen naar de module. Vervolgens kan dan via bluetooth dit worden uitgelezen met de app op een smartphone.

6.5 Zo wordt een simpele gebruikersomgeving rondom de digitale omgeving gemaakt.

De gebruikers omgeving moet modular zijn, aangezien er meerdere accounts zijn met verschillende rechten. Zo moet in de web interface makkelijk een module verborgen kunnen worden. Uiteindelijk is er gekozen voor web interface met 3 modules: Upload, Pending Blockchain, Definitieve Blockchain. De admin kan alle modules zien, de consensus alleen de pending en definitieve blockchain, de uploader kan alleen de upload module zien en de bekijkers kunnen alleen de definitieve blockchain zien.

De app moet ook simpel zijn en zal in de openingspagina een label hebben waar staat hoe je begint. Wanneer op de grote knop "Start scanning" wordt gedrukt zal er een lijst verschijnen met de bluetooth apparaten in de omgeving, de schip module zal gelijk opvallen en is ook de enige waarmee verbonden kan worden. Nadat de schip module via LoRa verbinding heeft gemaakt met de server wordt de blockchain opgehaald en vervolgens weergegeven. Als dit een lange blockchain is kan er door gescrollt worden. Een alternatieve app die WiFi gebruikt in plaats van LoRa is ook ontwikkelt. Deze werkt bijna precies hetzelfde maar nadat er is verbonden met blockchain zijn er twee velden voor de wifi naam en wifi wachtwoord die de gebruiker moet invullen. Als dit goed is gedaan wordt de blockchain weergegeven.

6.6 Hoe kan de naleving van de certificering van de IHM op schepen worden gewaarborgd en verbeterd met behulp van digitalisering technologieën?

De digitalisering technologie die de naleving van de certificering van de IHM waarborgen verbetert is blockchain. Met een blockchain systeem heb je de onveranderlijkheid, transparantie en gegevens integriteit die nodig is om de waarborging van de IHM te verbeteren. Door dit te combineren met andere technologieen zoals cloud servers, bluetooth en LoRa kan je dit verder uitbreiden door een robuust systeem te maken om de waarborging verder te verbeteren. Zo zal nu de blockchain altijd veilig staan op het cloud server dat goed te bereiken is met een webinterface voor de stakeholders. De schip module kan zelfstandig via Lora verbinden met de blockchain server. Dan met de app op een smartphone kan je over bluetooth de blockchain uitlezen.

Terugkijkend op de problemen en de vereiste voor dit systeem zie je dat het ontwikkelde prototype zodanig goed gerealiseerd is dat zo de naleving van de certificering van de IHM enorm verbeterd is.

Probleem 1, de onbetrouwbaarheid, is opgelost door de onveranderlijkheid van blockchain. Nadat een bestand (in een block) door de consensus stakeholder wordt goedgekeurd, waardoor zeker is dat de inhoud correct is, zal dit onaanpassbaar zijn. Het is onmogelijk in de web interface voor kwaadwillige om na het uploaden nog details in een bestand te veranderen. De enigste manier om dingen aan te passen is om in de server te haken. Maar de meest minuscule verandering zou al gedetecteerd worden door het hash-check algoritme.

Probleem 2, het versiebeheer, is opgelost door dit automatisch bij te houden in het blockchain systeem, bij elk block staan relevante details zoals de tijd, datum en gebruiker. Dit versiebeheer wordt zowel in de web interface als de schip module weergegeven. De tijd, naam van de gebruiker en datum worden allemaal automatisch gelogd zodat de gebruiker hier niet foutieve data kan invullen.

Probleem 3, Onveilige opslag van documenten is opgelost door gebruik te maken van een clouddserver. Een server die 24/7 aanstaat, altijd bereikbaar is en lang meegaat, veel handiger dan lokale opslag.

Probleem 4, toegang tot de documenten, is volledig verholpen door een gedeelde webinterface voor alle stakeholders. Via het internet is deze altijd bereikbaar als de gebruiker een account heeft gekregen. Het account systeem met verschillende privileges zorgt er ook voor dat belangrijke rechten zoals de consensus en uploaden beveiligd zijn voor bepaalde stakeholders.

Door niet alleen alle problemen op te lossen, maar ook verbeterde oplossingen te implementeren, is de naleving van de certificering van de IHM verbeterd met behulp van digitalisering technologieën.

7 Aanbevelingen

Enkele dingen waar dit project niet aan toe is gekomen, of andere functies die net buiten de scope vallen zijn te vinden hieronder.

DNV's IHM Manager (IHMM) biedt toegang voor meerdere schepen, oftewel meerde IHMs op hetzelfde server. Deze mogelijkheid zou waardevol zijn om ook aan de blockchain server toe te voegen. Hoewel er nog wel moet gekeken worden naar de overdraagbaarheid van de accounts, bijvoorbeeld of alleen de admin beide blockchains kan zien of dat de consensus ook oordeelt over beide blockchains. Wat hierbij ook besloten wordt, door het uitvoeren van meerdere websites op hetzelfde server zullen de onderhoudings kosten zeker gereduceerd worden.

Voor een goede LoRa verbinding vanuit de schip module moet de antenne zich buitenop het schip bevinden. Met als beste plek de antenne mast. LoRa kan grote afstanden overbruggen indien deze niet wordt afgeschermd, hoe hoger hoe beter. De schip module zelf kan op enkele plaatsen gemonteerd worden. De brug lijkt me de beste plek van het schip, want deze ligt vaak al vrij hoog en de kabel kan samen met de andere kabels voor de andere antenne's en radar's meegetrokken worden.

Two-factor authentication kan gebruikt worden voor het account systeem in de webinterface. Als een wachtwoord gecompromitteerd zou zijn, kan elke kwaadwillige gemakkelijk inloggen op dit account. Als dit account een consensus rol heeft, zou dit gebruikt kunnen worden om een vervalste IHM definitief op de blockchain te kunnen zetten. Daarom is het verstandig om elk account te binden aan een email, waar per inlog een code wordt verstuurd naar deze email om te verifiëren of deze persoon behoort tot dit account. Als je accounts aan een email bindt kunnen er ook emails gestuurd worden naar de desbetreffende stakeholders om deze te laten weet dat er een block moet worden goedgekeurd of dat er een nieuw block aan de definitieve blockchain is toegevoegd.

Voor de schaalbaarheid van dit product is het handig om de server omgeving te standaardiseren. Denk aan enkele veiligheidsmaatregelen die genomen moeten worden op elk server om zo de software beter te beschermen. Dit viel buiten de scope van deze opdracht, aangezien de focus lag op het ontwerpen van veilige software waarvan uitging dat die zich op een beveiligd server bevindt. Nu zou de server omgeving nog extra veiligheid maatregelen kunnen ondergaan. Denk aan bepaalde configuraties voor de ubuntu server om zo toegang tot de server beter te beveiligen.

De WiFi code en de LoRa code voor de microcontroller kunnen door een goede programmeur met wat tijd hopelijk gecombineerd worden. Zo zou de schip module LoRa en WiFi ondersteuning hebben. Als het omschrijven van de code niet mogelijk is, kan een andere microcontroller worden aangeschaft die wel genoeg flash geheugen heeft. Dan zou ook de code voor het opslaan van data in het flash geheugen hopelijk geïmplementeerd kunnen worden, want nu zorgde dat voor systeem crashes. Deze microcontroller zou wel een ESP32-chip moeten hebben of iets vergelijkbaar voor de bluetooth en WiFi functionaliteit. Een LoRa module zou apart aan de microcontroller kunnen worden aangesloten. Dat zou de behuizing iets groter maken maar omdat deze al erg compact is maakt het niet veel uit.

8 Bronnen

Referenties

- [1] In: (). URL: <https://www.thethingsnetwork.org/>.
- [2] Rahul Awati. „EEPROM (electrically erasable programmable read-only memory)”. In: (2022). URL: <https://www.techtarget.com/whatis/definition/EEPROM-electrically-erasable-programmable-read-only-memory>.
- [3] coinbase. „What is mining?” In: (2023). URL: <https://www.coinbase.com/learn/crypto-basics/what-is-mining>.
- [4] datalastic.com. „Ship Owners Types: A Comprehensive Overview”. In: (). URL: <https://datalastic.com/blog/ship-owners-types-a-comprehensive-overview>/.
- [5] DNV. „IHM and ship recycling”. In: *ihm-ship-recycling* (2024). URL: <https://www.dnv.com/maritime/insights/topics/ihm-ship-recycling/ihm-part-1-certification/>.
- [6] Joris Elfferich. „Hoe wordt de IHM digitaal beheerd in een veilige omgeving?” In: *HR* (2024), p. 8. URL: <http://145.24.223.204/>.
- [7] Joris Elfferich. „Hoe wordt de IHM gekoppeld aan een schip?” In: *HR* (2024), p. 8. URL: <http://145.24.223.204/>.
- [8] EMSA. „EMSA’s Best Practice Guidance on the Inventory of Hazardous Materials”. In: (2016). URL: <https://www.emsa.europa.eu/damage-stability-study/items.html?cid=77:publications&id=2874>.
- [9] Adam Hayes. „Radio Frequency Identification (RFID): What It Is, How It Works”. In: (2024). URL: <https://www.investopedia.com/terms/r/radio-frequency-identification-rfid.asp>.
- [10] Adam Hayes. „What Is a Blockchain?” In: (2023). URL: <https://www.investopedia.com/terms/b/blockchain.asp>.
- [11] Amy Hehemann. „Betekenis: Rederij”. In: (). URL: <https://theecomagency.nl/kennisbank/marketing/rederij/>.
- [12] Jesse Hollington. „What is NFC? How it works and what you can do with it”. In: (2023). URL: <https://www.digitaltrends.com/mobile/what-is-nfc/>.
- [13] IACS. „What are classification societies?” In: (). URL: <https://web.archive.org/web/20070119074545/http://www.eagle.org/company/Classmonograph.pdf>.
- [14] Wessel juristen. „Leverancier: een beknopte uitleg over leveranciers”. In: (). URL: <https://www.wesseljuristen.nl/ondernemingsrecht/leveranciers/>.
- [15] kinsta. „What Is GitHub?” In: (2023). URL: <https://kinsta.com/knowledgebase/what-is-github/>.
- [16] Lawinsider. „Ship recycling facility definition”. In: (2004). URL: <https://www.lawinsider.com/dictionary/ship-recycling-facility>.
- [17] Logos Logistics. „Wat is HAZMAT in de logistiek? Inzicht in veiligheid en compliance”. In: (2024). URL: <https://www.logos3pl.com/nl/what-is-hazmat-in-logistics-understanding-safety-and-compliance/>.

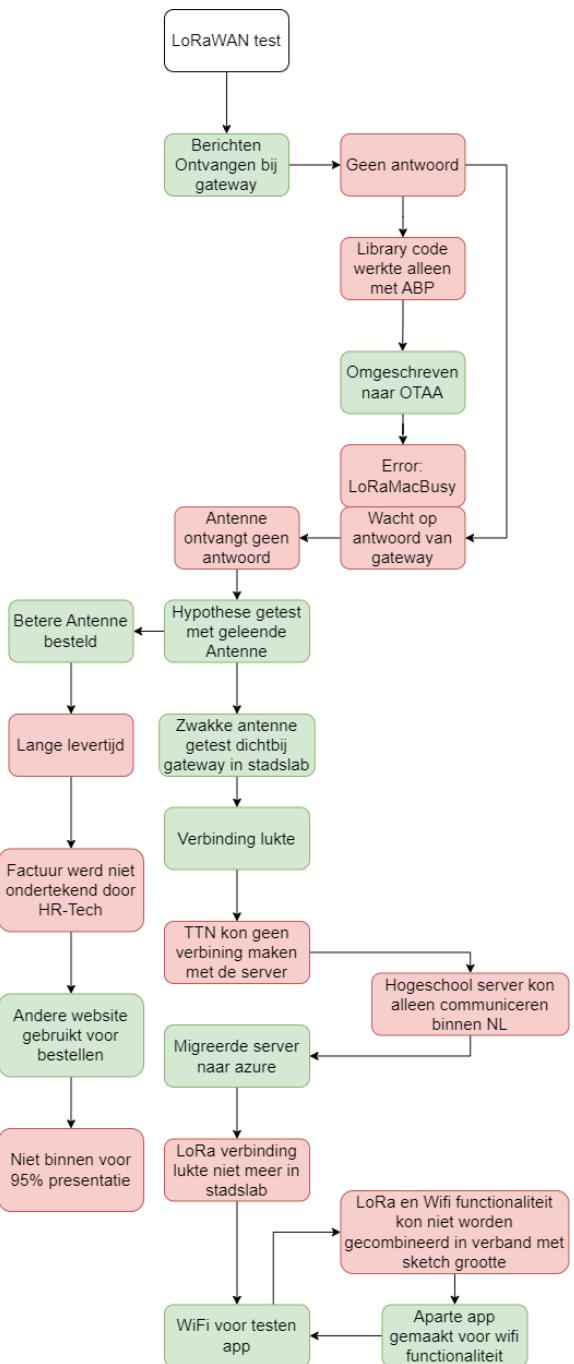
- [18] Ben Lutkevich. „DEFINITION: Database (DB)”. In: (2023). URL: <https://www.techtarget.com/searchdatamanagement/definition/database>.
- [19] Anuradha Malhotra. „Structure of a Bitcoin Block”. In: *Coinmonks* (2021). URL: <https://medium.com/coinmonks/structure-of-a-bitcoin-block-7f6c4938a5fd>.
- [20] Team MijnZZP. „SCHEEPSBOUWER, INFORMATIE OVER HET BEROEP, OPLEIDINGEN, COMPETENTIES”. In: (2024). URL: <https://www.mijnzzp.nl/Beroep/1271-Scheepsbouwer/Informatie>.
- [21] Scott Nevil. „What Is Proof of Work (PoW) in Blockchain?” In: (2023). URL: <https://www.investopedia.com/terms/p/proof-work.asp>.
- [22] Athanasios Pallis. „Chapter 4.2 – Port Authorities”. In: (). URL: <https://porteconomicsmanagement.org/pemp/contents/part4/port-authorities/>.
- [23] recfaces.com. „Biometric Devices — Complete Guide on Technology”. In: (2021). URL: <https://recfaces.com/articles/articles-biometric-devices>.
- [24] SHOBHIT SETH. „Public, Private, Permissioned Blockchains Compared”. In: (2023). URL: <https://www.investopedia.com/news/public-private-permissioned-blockchains-compared/>.
- [25] THE INVESTOPEDIA TEAM. „What Is a Hash? Hash Functions and Cryptocurrency Mining”. In: (2023). URL: <https://www.investopedia.com/terms/h/hash.asp>.
- [26] thethingsnetwork. „What are LoRa and LoRaWAN?” In: (). URL: <https://www.thethingsnetwork.org/docs/lorawan/what-is-lorawan/>.
- [27] Melanie Uy. „What Is Bluetooth?” In: (2022). URL: <https://www.lifewire.com/what-is-bluetooth-2377412>.
- [28] vmware. „What is a cloud server?” In: (). URL: <https://www.vmware.com/topics/glossary/content/cloud-server.html>.

9 Bijlage

9.1 Progress Flow

De factory test example code werkte wel op de microcontroller, maar de LoRaWAN voorbeeld code werkte niet. Wat ging er fout? Door de microcontroller te linken met TTN (the things network) was er in de console te zien dat er wel degelijke LoRaWAN join requests werden gestuurd vanuit dit apparaat en dat de join request werd geaccepteerd door het systeem. Maar de data kwam niet aan. Daarom werd het join request na enkele seconden weer opnieuw gestuurd. Aangezien heltec deze code zelf had geschreven met een herschreven geimporteerde libraries voor dit specifieke bord was het moeilijk om te achterhalen wat er nou fout ging. De arduino code was kort en verwees naar de LoRaWAN-APP.c library. Hierin gebeurde eigenlijk het hele LoRa proces. Door meerdere print statements te gebruiken was er te achterhalen wat er mis ging. Zo bleef de switch statement vast blijven in de sleep case, terwijl de interrupt die de informatie zou versturen nooit werd aangezet. Na wat zoeken vond ik een if statement dat een bool gebruikte die alleen bij de ABP (Activation By Personalization) wordt overschreven, terwijl tegenwoordig bijna alleen maar OTAA (Over-The-Air Activation) wordt gebruikt. Ik heb daarom een nieuwe bool aangemaakt die op true wordt gezet nadat de join functie is afgerond via OTAA. Nu wordt eindelijk de send functie goed aangeroepen maar de data komt nogsteeds niet goed aan. De send functie roept LoRaMacMcpsRequest() aan, deze bevindt zich weer in een andere library genaamd LoRaMac.c. Door ook in deze library print statements aan te roepen zag ik dat altijd LORAMAC-STATUS-BUSY werd gereturned. Aannemelijk omdat de microcontroller nog wacht op een ack van de LoRaWAN gateway. Het probleem was dus dat de gateway wel het signaal kreeg, maar de module het antwoord niet ontving. Of dit kwam door een fout in de code/module of door de connectiviteit bleek onduidelijk. Testen in hof van Delft kreeg ik niks te zien op de TTN, TU Delft ook niet. Alleen bij HRTech zag ik in de TTN console dat de Join request was ontvangen. Er ontstond een hypothese dat de standaard antenne niet goed genoeg was om het signaal van de gateway kilometers verderop te ontvangen. Op het RDM heb ik bij RAAST de antenne geleend die wordt gebruikt voor hun AIS systeem. Deze was een stuk groter en hiermee werden de join-accept berichten eindelijk ontvangen door de antenne en zo kon de microcontroller dus een verbinding opleggen met het LoRaWAN netwerk. Nu was vastgesteld dat de huidige antenne niet goed genoeg was voor een verbinding met het LoRaWAN netwerk moest er gekeken worden naar het aanschaffen van een betere antenne....

Voorlopig werkte de huidige antenne alleen als die zicht dichtbij een gateway bevond. Zo was er bij het stadslab van de Hogeschool Rotterdam, Wijnhaven 101, een LoRaWAN gateway. Door de antenne te plaatsen in het stadslab kon dus verbinding gemaakt worden met The Things Network. De microcontroller stuurt nadat deze succesvol is verbonden met de gateway een berichtje, via dit berichtje wordt een webhook aangeroepen. Deze webhook stuurt een HTTP request naar de blockchain server. Maar toen ik dit testen werkte dit niet. De TTN console liet zien dat er geen bericht gestuurd kon worden naar de blockchain server. Mijn laptop en telefoon konden wel verbinding maken met de blockchain server dus de hypothese was dat de fout lag bij TTN. Maar na alles na te gaan zou TTN goed geconfigureerd moeten zijn. Toen ontstond de hypothese dat alleen Nederlandse verbindingen werden toegelaten bij de blockchain server. Deze hypothese werd gevalideerd toen ik met mijn VPN vanuit Duitsland het server probeerde te bereiken. Na het berichten van de server beheerder bleek dat de servers van de Hogeschool Rotterdam geen internationale verbindingen accepteerde en dit kon niet voor mij aangepast worden. Nu moest er dus een ander server gebruikt worden als er verbinding gemaakt wilt worden met TTN. Hier volgt een flowchart die in rood tegenslagen laat zien en in het groen de oplossingen: 9



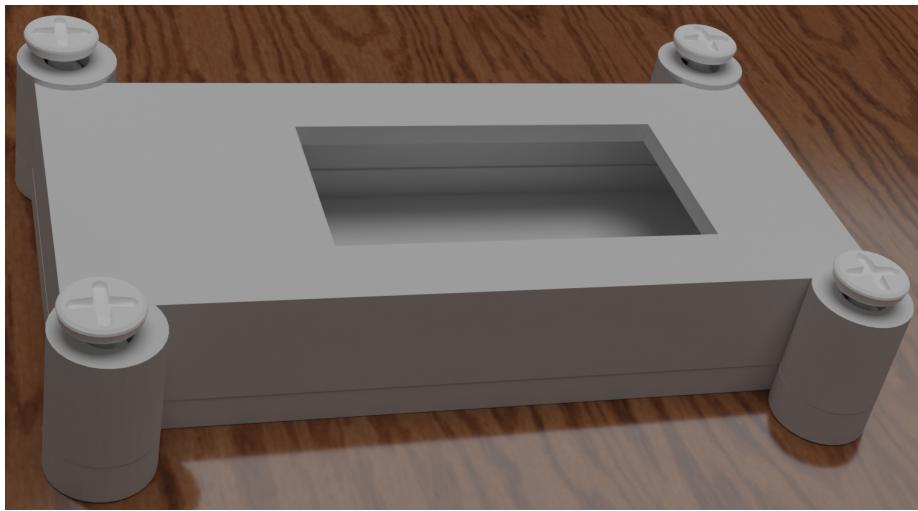
Figuur 9: Progress-flow

			Hazardous Material	Threshold Value*
Annex I to the EU SRR	Appendix 1 to the HKC /	Table A of the Res. MEPC.379(80)	Asbestos ¹	0.10%
			Ozone-depleting substances (ODS) ²	No threshold value
			Polychlorinated biphenyls (PCB)	50 mg/kg
			Anti-fouling systems containing organotin	2500 mg total tin/kg
			Anti-fouling systems containing cybutryne	1000 mg/kg
			Perfluoroctane sulfonic acid (PFOS) ³	10 mg/kg
Annex II to the EU SRR	Appendix 2 to the HKC	Table B of the Res. MEPC.379(80)	1. Any hazardous materials listed in Annex I / Appendix 1	
			2. Cadmium and Cadmium Compounds	100 mg/kg
			3. Hexavalent Chromium and Hexavalent Chromium Compounds	1000 mg/kg
			4. Lead and Lead Compounds	1000 mg/kg
			5. Mercury and Mercury Compounds	1000 mg/kg
			6. Polybrominated Biphenyl (PBBs)	50 mg/kg
			7. Polybrominated Diphenyl Ethers (PBDEs)	1000 mg/kg
			8. Polychlorinated Naphthalenes (more than 3 chlorine atoms)	50 mg/kg
			9. Radioactive Substances	No threshold value
			10. Certain Short chain Chlorinated Paraffin (Alkanes, C10-C13, chloro)	1%
			11. Brominated Flame Retardant (HBCDD)	100 mg/kg

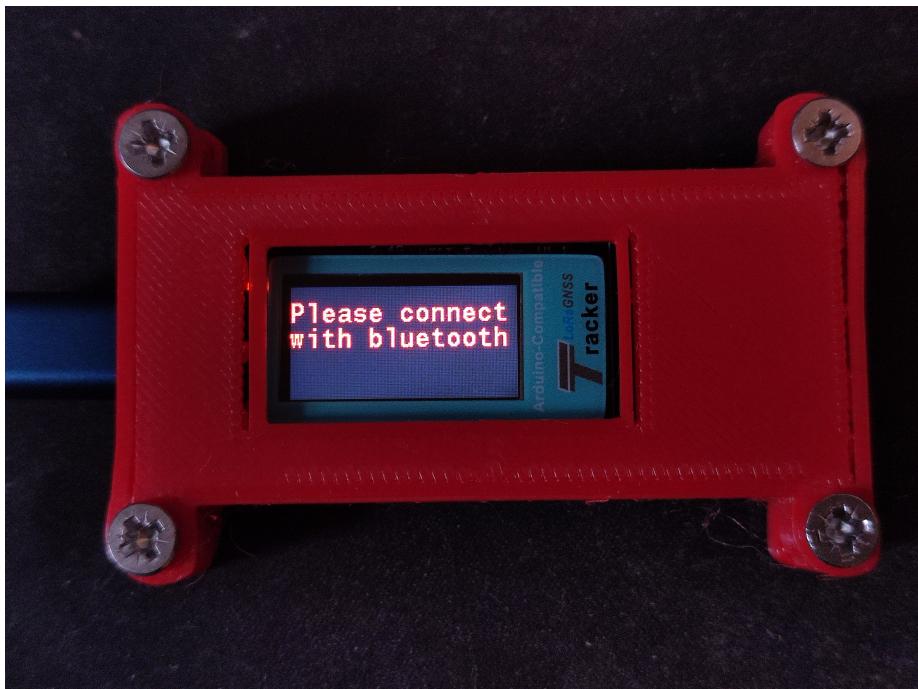
Figuur 10: Hazardous Materials

Scope of the IHM		Shipbuilding & Operation	Preparation prior to Recycling		
HKC	EU SRR		Part I Structure & Equipment	Part II Operationally generated Wastes	Part III Stores
Appendix 1	Annex I	✓			
Mandatory for new / existing ships & new installations					
Appendix 2	Annex II	✓			
Mandatory for new ships / installations; as far as practicable for existing ships					
Table C Materials Potentially hazardous items				✓	✓
Table D Materials Regular consumable goods potentially containing hazardous materials					✓

Figuur 11: Inventory of Hazardous Materials, Part I, II en III



Figuur 12: 3D Render van behuizing



Figuur 13: Gerealiseerde behuizing

The screenshot shows a web browser window with a header bar containing 'New Tab', 'Import bookmarks...', and 'Getting Started'. Below the header, the page title is 'Blockchain Network' with links for 'Create Account' and 'Change Password'. The main content area has three main sections:

- Upload File**: A form field with a placeholder 'Enter description:'.
- Pending Files**: A table-like structure with columns for 'User Name', 'File Name & (Timestamp) --> Download', and 'File description:'. It includes 'Approve' and 'Disapprove' buttons.
- Uploaded Files**: A table-like structure with columns for 'User Name', 'File Name & (Timestamp) --> Download', and 'File description:'.

At the bottom left is a 'Submit' button.

Figuur 14: Website Design Optie A

The screenshot shows a web browser window with a header bar containing 'New Tab', 'Import bookmarks...', and 'Getting Started'. Below the header, the page title is 'Blockchain Network' with links for 'Create Account' and 'Change Password'. The main content area has three main sections:

- Upload File**: A form field with a placeholder 'Enter description:'.
- Pending Files**: A table-like structure with columns for 'User Name', 'File Name & (Timestamp) --> Download', and 'File description:'. It includes 'Approve' and 'Disapprove' buttons.
- Uploaded Files**: A table-like structure with columns for 'User Name', 'File Name & (Timestamp) --> Download', and 'File description:'.

At the bottom left is a 'Submit' button.

Figuur 15: Website Design Optie B

The screenshot shows a web application window titled "Blockchain Network". At the top, there are links for "Create Account" and "Change Password".

Upload File:

- Description:
- Upload File:
- Submit

Pending Files:

User Name	<File Name> (Timestamp) -> Download	File description:
		<input type="button" value="Approve"/> <input type="button" value="Disapprove"/>

Uploaded Files:

User Name	<File Name> (Timestamp) -> Download	File description:

Figuur 16: Website Design Optie C