Literatuur Onderzoek: Software

# Inleiding

Voor het digitaliseren van het IHM moet deze veilig worden opgeslagen. Maar hoe slaan we de IHM op? Er zijn veel verschillende manieren, en we moeten kijken welke oplossing het beste pas bij de requirements van de IHM. De requirements zijn terug te vinden in de Req\_Analyse.

# Wat moet er opgeslagen worden?

De IHM (Inventory of Hazardous Materials) is een document dat een cruciaal onderdeel is van de maritieme industrie, met name in de context van scheepsrecycling. Het biedt een gedetailleerd overzicht van alle gevaarlijke materialen die aanwezig zijn op het schip. Dit is essentieel voor het waarborgen van veiligheid, milieubescherming en naleving van internationale regelgeving zoals de Hong Kong Conventie en de EU-regelgeving over scheepsrecycling (Ren Di & Lougridis, 2021).

Nauwkeurigheid in de IHM is van het grootste belang. Een incorrecte IHM kan leiden tot veiligheidsrisico's, milieuschade en niet-naleving van regelgeving, wat kostbaar of gevaarlijk kan zijn. Als bijvoorbeeld een gevaarlijk materiaal niet correct wordt geïdentificeerd en gedocumenteerd, kan het onjuist worden behandeld tijdens de scheepsrecycling, wat potentieel schadelijk kan zijn voor werknemers en het milieu.

Beveiliging van de IHM is dus erg belangrijk. Door de gevoeligheid van de informatie, is het cruciaal om ervoor te zorgen dat deze veilig wordt opgeslagen en alleen kan worden aangepast door geautoriseerd personeel. Ongeautoriseerde toegang tot of manipulatie van de IHM-gegevens kan leiden tot onjuiste behandeling van gevaarlijke materialen, met mogelijke veiligheids- en milieugevolgen.

De IHM is een document van x pagina’s lang….

# Opties:

Er zijn veel manieren op bestanden op te slaan, hier kijken we naar wat populaire opties en of deze bij de requirements past:

## Database:

Databases zijn de meest gebruikte manier om grote aantallen data op te slaan. Deze database kan zowel lokaal en in de cloud worden opgeslagen. In de cloud opslaan zorgt ervoor dat je overal bij de database kan. Handig maar dat betekent ook dat je kan worden aangevallen door cyberattacks. Lokaal opslaan op een (micro)computer zou veiliger kunnen zijn. Dan zou je echt de data alleen kunnen ophalen of aanpassen op het schip waarvan de IHM is. Voor zowel een cloud en lokale database zou je een database administrator nodig hebben die deze database beheert en beveiligd. Ook zullen er verschillende user accounts moeten worden gemaakt voor de verschillende autoriteiten die moeten kunnen valideren of aanpassen. De beveiliging bij de database beheerder leggen kan ook voor zwakheden in de beveiliging zorgen. De IHM is ook een document in hetzelfde formaat als een tekstdocument. Als je deze in een database wilt zetten zou je ook nog een nieuwe database moeten maken die lijkt op het oorspronkelijke document.

## Lokaal opslaan:

Vrijwel de meest simpele oplossing aan de software kant. Hier is het idee dat er op het schip een (micro) computer wordt geplaatst. Vervolgens met behulp van een speciaal programma of de ingebouwde OS-beveiliging wordt de IHS beveiligd met een wachtwoord of token (gekoppeld aan een speciale pas). Zo kan deze alleen worden aangepast door mensen met de juiste autorisatie. Deze oplossing is niet schaalbaar, niet superveilig en misschien wat onhandig. Hier zou het IHM een tekstdocument zijn wat makkelijk aan te passen is. Maar dat betekent dat alle aanpassingen gedaan moeten worden op het schip zelf. Dit kan onhandig zijn. In principe hoef je op het schip alleen de aanpassingen aan het IHM te moeten kunnen zien en of het IHM aanwezig is. Aanpassingen aan het IHM zouden beter digitaal gemaakt kunnen worden via het internet.

## Blockchain:

Implementeer een blockchain-systeem voor het bijhouden van de IHM. Blockchain biedt een gedecentraliseerd en transparant register waarin alle wijzigingen traceerbaar en onveranderlijk zijn. Dit zorgt voor betrouwbaarheid en integriteit van de gegevens. Elke wijziging moet worden gevalideerd door meerdere partijen, waardoor frauduleuze manipulatie wordt voorkomen. Hier wordt de IHM dus opgeslagen en ge-encrpyt alleen de hash van het document wordt opgeslagen in de blockchain. Voor elke aanpassing wordt een nieuwe versie van het document gemaakt, van dit document wordt ook een hash gemaakt en deze word gechained aan de vorige hash. Zo zul je een opeenvolgend record krijgen van alle aanpassingen van het document, wat erg goed is voor valideren en verifiëren van wijzigingen.

CLOUD/IPFS:

# Afweging

Op deze 3 opties na zijn er niet veel andere alternatieven om het op te slaan. Dus we moeten hieruit een beslissing maken. Of misschien hoeft dat niet? We kunnen namelijk een combinatie gebruiken. Alhoewel we de IHM direct in de blockchain kunnen opslaan is het gebruiken van een hash toch wat sneller. Dan zou de IHM toch beveiligd lokaal opgeslagen zijn, maar alleen toegankelijk met de hash uit de blockchain. Waarschijnlijk zit er ook een database aangekoppeld met ID’s die toegang hebben tot het maken van aanpassingen. Blockchain zal dan nog steeds wel centraal liggen als de manier om de IHM veilig op te slaan, maar ondersteunend door de andere opties.

# Blockchain: private, public of hybride

Er zijn een paar verschillende types blockchain netwerken.

Public:  
In dit netwerk kan iedereen meedoen met het netwerk. Binnen dit netwerk kan iedereen lezen, schrijven en valideren. Bij publieke blockchains, zoals Bitcoin en Ethereum, zijn alle transacties volledig transparant. Dit draagt bij aan de traceerbaarheid en verifieerbaarheid van transacties. Dit maakt het netwerk erg gedecentraliseerd. Binnen een public netwerk willen nieuwe deelnemers meedoen om het te gebruiken binnen hun eigen doeleinden. Hoe meer mensen er deelnemen des te veiliger het is. Blockchain werkt namelijk peer to peer, en hoe meer peers er zijn, hoe veiliger het is. Deelnemers krijgen ook een prijs voor elke validatie ze maken voor andere mensen binnen het netwerk. De prijs die deelnemers krijgen, vaak 'mining reward' genoemd, om mensen te stimuleren voor het onderhouden van de netwerkintegriteit Bij dit valideren komen wel gegevens vrij zoals de inhoud en de adressen, hierdoor kan je anonimiteit verliezen.

### Private:

Deelnemers kunnen alleen deelnemen aan dit netwerk door een uitnodiging, zodat de identiteit van alle deelnemers vast is gesteld. Private blockchains worden vaak gebruikt in bedrijfsomgevingen waar controle over de deelnemers en activiteiten essentieel is. Binnen dit netwerk wordt er gecontroleerd wie mag valideren (minen) en wie meedoet aan de consensus protocollen. Hoewel private blockchains minder gedecentraliseerd zijn, kunnen ze aanzienlijk efficiënter zijn in transactiesnelheid en energieverbruik. Je kan het meer zien als een gesloten database beveilidg met crypto grafische sleutels. Alleen mensen met toestemming in dit netwerk mogen aanpassingen maken en gegevens valideren. Private blockchains geven dus prioriteit aan efficiëntie en onveranderlijkheid. Maar omdat er minder mensen toegang hebben zijn er dus minder validaties wat het netwerk onveiliger maakt met betrekking tot datalekken. Ook is er misschien geen sprake van consensus, maar alleen van de onveranderlijkheid van de ingevoerde gegevens.

Hybride:  
Dit blockchain netwerk is een mix tussen private and public. Iedereen kan deelnemen nadat de identiteit is geverifieerd. Zo krijgen de deelnemers alleen permissies om specifieke activiteiten uit te voeren (lezen, schrijven of invoeren). Hybride blockchains kunnen dus meerdere functies hebben, en wordt vaak gemaakt en verhuurd aan bedrijven die de voordelen van zowel publieke als private netwerken willen benutten, zoals transparantie en controle over bepaalde aspecten van de blockchain. De beveiligingsaspecten van hybride blockchains hangen af van de specifieke architectuur en implementatie. Maar ze zijn over het algemeen veiliger dan publieke netwerken, hoewel het risico op hacking is nog steeds aanwezig, net als bij alle onlinesystemen.

Conclusie:  
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 prive 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 prive netwerk sneller en makkelijker zijn om te ontwikkelen, en biedt de juiste vereiste voor de opdracht omschrijving.

# Hoe slaan we de IHM op in de blockchain?

De IHM is een vrij groot bestand, hoe slaan we deze op?

**Direct in blockchain:**  
Het is mogelijk om een bestand op te slaan in een blockchain blok. Voor grotere bestanden krijg je dan wel latency bij het ophalen van een block. Dit zorgt wel voor een erg veilige dataopslag waar de eerste versie van de IHM nooit aangepast kan worden en altijd weer opgehaald kan worden. Aanpassingen moeten dan gechained worden aan het eerste block en zo kan je altijd de bestanden met elkaar vergelijken. Wanneer de blockchain langer wordt zal het ophalen ook langer duren.

**Hash in blockchain:**Door de hash van een bestand op te slaan in de blockchain is het systeem sneller want de grote van het bestand van een hash is veel kleiner. Wat is een hash? Een hash is een ge-encodeerde indruk van een bestand in text. Dit reflecteert de inhoud van de bestand, een miniscule aanpassing aan het bestand zal voor een andere hash zorgen. Door de hash in de blockchain op te slaan. Als je later wilt kijken of de IHM (opgeslagen op een server) niet aangepast is kan je een nieuwe hash genereren en die vergelijken met de oorspronkelijke, als deze hetzelfde is dan is de IHM nog valide. Als de hash nu anders is, zal er iets aan de inhoud veranderd zijn.

De IHM direct in de blockchain zetten is een makkelijke veilige oplossing maar zal minder snel zijn. Alleen hashes gebruiken is sneller, maar zal extra veiligheidsmaatregelen nodig hebben om extra veilig te zijn. Zo zou er regelmatig gekeken moeten worden of de hash in blockchain hetzelfde is als de hash van het huidige bestand om veranderingen in de IHM te identificeren. Ook zou er een backup moeten worden gemaakt want als de IHM wordt aangepast kan je met de blockchain hash niet het bestand recreëren. Om vast te stellen welke mogelijkheid beter is zal er een experimenteel onderzoek moeten worden uitgevoerd om vast te stellen welke methode beter is.

Consensus niet op schip

Validatie en certification validation is anders.

certification validation stempel in blockchain

### google & apple wallet voor NFC?

Alhoewel een telefoon via apple of google wallet een NFC card kan na bootsen, is dit niet zo simpel. Je kan niet zomaar een zelf gecustomizeerde NFC kaart aan een wallet toevoegen, want google vereist eerst een agreement voordat je een kaart kan toevoegen. Hetzelfde geldt voor Apple. Je zou via een andere app de NFC functionaliteit kunnen proberen te gebruiken maar hier komen ook vaak problemen mee. Ten eerste zal je de telefoon moeten rootten, dit omdat NFC kaart ID naar de configuratie van de telefoon moet worden gestuurd waarvoor root privileges nodig voor zijn. Deze stap is te onhandig voor de gebruikers en er zal dus naar een alternatief moeten worden gekeken.

Alleen veranderingen in de IHM module.

Kijk IHM procedure hoe veranderingen eruit zien

aanbeveling: port authority check IHM aanwezig en correct?

Bronnen

<https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:330:0001:0020:EN:PDF>

<https://mitsloan.mit.edu/ideas-made-to-matter/blockchain-explained>

<https://www.investopedia.com/terms/b/blockchain.asp>

<https://www.investopedia.com/news/public-private-permissioned-blockchains-compared/>

<https://www.jsign.com/blog/storing-documents-with-blockchain>

|  |  |  |
| --- | --- | --- |
| Versie | Verandering | Datum |
| 0.1 | Opzet gemaakt | 06/02/24 |