

ANALYSING SOUP

BAS BRUNINK



Een weg naar veiligere software

Software Engineering

FDMCI

Hogeschool van Amsterdam

Februari 2022 – version 0.1

SAMENVATING

Short summary of the contents... a great guide by Kent Beck how to write good abstracts can be found here:

<https://plg.uwaterloo.ca/~migod/research/beck00PSLA.html>

INHOUDSOPGAVE

LIJST VAN FIGUREN

LIJST VAN TABELLEN

LISTINGS

ACRONIEMEN

API	Application Programming Interface
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CTO	Chief Technology Officer
OSS	Open Source Software
OTAP	Ontwikkeling Test Acceptatie Productie
SOUP	Software of Unknown Pedigree / Provenance
UML	Unified Modeling Language

Het document dat voor u ligt is een resultaat van een onderzoek en product oplevering als afstudeeropdracht door Bas Brunink voor het bedrijf Eaglescience. Het zal het process beschrijven die ik gelopen heb om een module te schrijven die automatisch een SOUP analyse doet op zowel bestaande als nieuwe projecten.

1.1 LEESWIJZER

Deze scriptie neemt de lezer mee door het verloop van het project van idee tot implementatie. Met als einde een resultaat beschrijven en een prognose in de verbetering gezien de verwachting is dat er niet direct een significante verbetering te zien is.

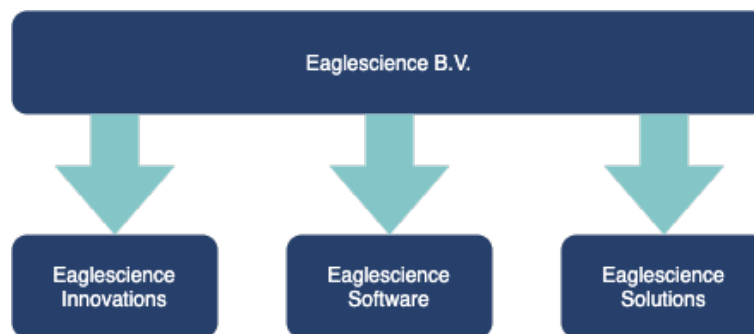
Deel I

OPDRACHT

Het hier beschreven onderzoek en daarbij behorende applicatie is geschreven in opdracht van Eaglescience wat gevestigd is in Amsterdam Sloterdijk. Eaglescience ontwikkeld complexe software op projectbasis voor diverse klanten vaak met een wetenschappelijke inslag. Het bedrijf telt +/- 20 medewerkers waarvan 75% ontwikkelaar/designer zijn en de resterende 25% een support rol bekleden (project managers finance manager, Quality manager) Aan het hoofd van Eaglescience staat een CEO, Marc Grootjen, CTO Bas Breier, CFO Wender van Mansvelt. Naast het ontwikkelen van nieuwe software biedt Eaglescience ook de mogelijkheid om zorg te dragen voor de eventuele hosting van het opgeleverde product. Hiermee kan Eaglescience nog beter garanderen dat de geboden kwaliteit in de software gewaarborgd blijft tijdens de levensduur van de software.

2.1 ORGANISATIE

Eaglescience bestaat uit drie divisies die elk onder Eaglescience B.V. vallen. Iedere divisie is verantwoordelijk voor een deel van die diensten die Eaglescience aanbied.



Figuur 1: Organogram Eaglescience

2.2 MISSIE

De missie van Eaglescience is het bedienen van onze partners door een ontwerp, ontwikkeling en service te bieden op het gebied van op maat gemaakte IT oplossingen. Om dit te kunnen bewerkstelligen heeft Eaglescience goed opgeleide IT professionals in dienst die zichzelf continue ontwikkelen op de “cutting edge” van IT technologie. De hoofd competenties van de medewerkers zijn: innovatief, intelligent, klant geïnteresseerd, flexibel en ambitieus.

2.3 VISIE

Eaglescience streeft er als innovatief IT bedrijf naar om software te ontwikkelen als een Business-to-Business dienst. Met onze technische vaardigheden bouwen we veilige en hoogwaardige software die bijdraagt aan een betere wereld. Omdat we agile werken, leveren we precies wat nodig is, niets meer en niets minder. Wij helpen onze klanten zoeken naar een langdurige betrokkenheid en samenwerking op basis van zowel vertrouwen als wederzijds respect. Omdat elke vraag uniek is, ontwikkeld Eaglescience op maat gemaakte en innovatieve software. We zijn van plan deel uit te maken van het hele proces van het formuleren van een idee tot het lanceren van het product en het waarborgen van de productie levenscyclus. Onze belangrijkste succesfactor zijn de mensen, die zich continu ontwikkelen door met de nieuwste technieken te werken op diverse projecten. Wij streven naar een optimale

balans tussen werk en privé. Dit geeft onze medewerkers veel vrijheid, maar vereist zelfdiscipline en verantwoordelijkheid.

2.4 STRATEGIE

strategische thema's

Eaglescience levert de visie via vier strategische thema's:

- Maatschappelijke verantwoordelijkheid
- Persoonlijke groei
- Tevredenheid

We streven ernaar om veilige en hoogwaardige software diensten te leveren die waarde toevoegen aan onze samenleving. We streven naar een bedrijfscultuur waarin alle collega's hun talenten kunnen laten groeien. We hebben een ongecompliceerd werkethos: we richten ons op resultaten van hoge kwaliteit, maar met een gezonde balans tussen werk en privé en voldoende tijd voor leuke en sociale evenementen. Eaglescience verwacht van alle medewerkers dat zij hun handelen baseren op vier kwaliteitsprincipes:

- Meld situaties die niet voldoen aan onze interne procedures
- Evaluer risico's wanneer grote veranderingen worden verwacht
- Help en daag elkaar uit
- Kennis behouden over compliancy en kwaliteitsmanagement

2.5 RELEVANTE EN ACTUELE ONTWIKKELINGEN BINNEN EAGLESCIENCE

Eaglescience is aan het groeien, zowel in het aantal projecten waar aan gewerkt wordt als het aantal medewerkers. Daarnaast worden de diensten die Eaglescience aanbied ook uitgebreid. Waarbij het hosten van de ontwikkelde applicaties steeds meer wordt aangeboden. Door deze inzet ligt de verantwoordelijk niet alleen bij het leveren van een veilige en hoogwaardige software maar het leveren van service waarbij de applicaties in een veilige omgeving worden aangeboden. Mede door de groei van het bedrijf maar zeker ook de diensten die aangeboden wordt is het zeer relevant om taken die geautomatiseerd kunnen worden te automatiseren.

EXAMPLES

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetur id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

3.1 A NEW SECTION

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Examples: *Italics*, ALL CAPS, SMALL CAPS, LOW SMALL CAPS¹. Acronym testing: UML! (UML!) – UML! – UML! (UML!) – UMLs

3.1.1 Test for a Subsection

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetur adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula.

Fusce mauris. Vestibulum luctus nibh at lectus. Sed bibendum, nulla a faucibus semper, leo velit ultricies tellus, ac venenatis arcu wisi vel nisl. Vestibulum diam. Aliquam pellentesque, augue quis sagittis posuere, turpis lacus congue quam, in hendrerit risus eros eget felis. Maecenas eget erat in sapien mattis porttitor. Vestibulum porttitor. Nulla facilisi. Sed a turpis eu lacus commodo facilisis. Morbi fringilla, wisi in dignissim interdum, justo lectus sagittis dui, et vehicula libero dui cursus dui. Mauris tempor ligula sed lacus. Duis cursus enim ut augue. Cras ac magna. Cras nulla. Nulla egestas. Curabitur a leo. Quisque egestas wisi eget nunc. Nam feugiat lacus vel est. Curabitur consectetur.

Note: The content of this chapter is just some dummy text.

¹ Footnote example.

3.1.2 *Autem Timeam*

Suspendisse vel felis. Ut lorem lorem, interdum eu, tincidunt sit amet, laoreet vitae, arcu. Aenean faucibus pede eu ante. Praesent enim elit, rutrum at, molestie non, nonummy vel, nisl. Ut lectus eros, malesuada sit amet, fermentum eu, sodales cursus, magna. Donec eu purus. Quisque vehicula, urna sed ultricies auctor, pede lorem egestas dui, et convallis elit erat sed nulla. Donec luctus. Curabitur et nunc. Aliquam dolor odio, commodo pretium, ultricies non, pharetra in, velit. Integer arcu est, nonummy in, fermentum faucibus, egestas vel, odio.

3.2 ANOTHER SECTION IN THIS CHAPTER

Sed commodo posuere pede. Mauris ut est. Ut quis purus. Sed ac odio. Sed vehicula hendrerit sem. Duis non odio. Morbi ut dui. Sed accumsan risus eget odio. In hac habitasse platea dictumst. Pellentesque non elit. Fusce sed justo eu urna porta tincidunt. Mauris felis odio, sollicitudin sed, volutpat a, ornare ac, erat. Morbi quis dolor. Donec pellentesque, erat ac sagittis semper, nunc dui lobortis purus, quis congue purus metus ultricies tellus. Proin et quam. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Praesent sapien turpis, fermentum vel, eleifend faucibus, vehicula eu, lacus.

Sia ma sine svedese americas. Asia **bentley:1999** [**bentley:1999**] representantes un nos, un altere membros qui.² Medical representantes al uso, con lo unic vocabulos, tu peano esencialmente qui. Lo malo laborava anteriormente uso.

DESCRIPTION-LABEL TEST: Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Donec odio elit, dictum in, hendrerit sit amet, egestas sed, leo. Praesent feugiat sapien aliquet odio. Integer vitae justo. Aliquam vestibulum fringilla lorem. Sed neque lectus, consectetur at, consectetur sed, eleifend ac, lectus. Nulla facilisi. Pellentesque eget lectus. Proin eu metus. Sed porttitor. In hac habitasse platea dictumst. Suspendisse eu lectus. Ut mi mi, lacinia sit amet, placerat et, mollis vitae, dui. Sed ante tellus, tristique ut, iaculis eu, malesuada ac, dui. Mauris nibh leo, facilisis non, adipiscing quis, ultrices a, dui.

LABEL TEST 2: Morbi luctus, wisi viverra faucibus pretium, nibh est placerat odio, nec commodo wisi enim eget quam. Quisque libero justo, consectetur a, feugiat vitae, porttitor eu, libero. Suspendisse sed mauris vitae elit sollicitudin malesuada. Maecenas ultricies eros sit amet ante. Ut venenatis velit. Maecenas sed mi eget dui varius euismod. Phasellus aliquet volutpat odio. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Pellentesque sit amet pede ac sem eleifend consectetur. Nullam elementum, urna vel imperdiet sodales, elit ipsum pharetra ligula, ac pretium ante justo a nulla. Curabitur tristique arcu eu metus. Vestibulum lectus. Proin mauris. Proin eu nunc eu urna hendrerit faucibus. Aliquam auctor, pede consequat laoreet varius, eros tellus scelerisque quam, pellentesque hendrerit ipsum dolor sed augue. Nulla nec lacus.

This statement requires citation **cormen:2001** [**cormen:2001**].

3.2.1 *Personas Initialmente*

Suspendisse vitae elit. Aliquam arcu neque, ornare in, ullamcorper quis, commodo eu, libero. Fusce sagittis erat at erat tristique mollis. Maecenas sapien libero, molestie et, lobortis in, sodales eget, dui. Morbi ultrices rutrum lorem. Nam elementum ullamcorper leo. Morbi dui. Aliquam sagittis. Nunc placerat. Pellentesque tristique sodales est. Maecenas imperdiet lacinia velit. Cras non urna. Morbi eros pede, suscipit ac, varius vel, egestas non, eros. Praesent malesuada, diam id pretium elementum, eros sem dictum tortor, vel consectetur odio sem sed wisi.

² De web nostre historia angloromanic.

LABITUR BONORUM PRI NO	QUE VISTA	HUMAN
fastidii ea ius	germano	demonstratea
suscipit instructor	titulo	personas
quaestio philosophia	facto	demonstrated knuth:1976

Tabel 1: Autem timeam deleniti usu id. **knuth:1976**

3.2.1.1 A Subsubsection

Sed feugiat. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Ut pellentesque augue sed urna. Vestibulum diam eros, fringilla et, consectetur eu, nonummy id, sapien. Nullam at lectus. In sagittis ultrices mauris. Curabitur malesuada erat sit amet massa. Fusce blandit. Aliquam erat volutpat. Aliquam euismod. Aenean vel lectus. Nunc imperdiet justo nec dolor.

A PARAGRAPH EXAMPLE Etiam euismod. Fusce facilisis lacinia dui. Suspendisse potenti. In mi erat, cursus id, nonummy sed, ullamcorper eget, sapien. Praesent pretium, magna in eleifend egestas, pede pede pretium lorem, quis consectetur tortor sapien facilisis magna. Mauris quis magna varius nulla scelerisque imperdiet. Aliquam non quam. Aliquam porttitor quam a lacus. Praesent vel arcu ut tortor cursus volutpat. In vitae pede quis diam bibendum placerat. Fusce elementum convallis neque. Sed dolor orci, scelerisque ac, dapibus nec, ultricies ut, mi. Duis nec dui quis leo sagittis commodo.

- A. Enumeration with small caps
- B. Second item

A PARAGRAPH EXAMPLE Uno de miembros summario preparation, es inter disuso qualcunqu que. Del hodie philologos occidental al, como publicate litteratura in web. Veni americano **knuth:1976** [**knuth:1976**] es con, non internet millennios secundarimente ha. Titulo utilitate tentation duo ha, il via tres secundarimente, uso americano inicialmente ma. De duo deler personas inicialmente. Se duce facite westeuropae web, ?? nos clave articulos ha. Another statement requiring citation **sommerville:1992** [**sommerville:1992**] but this time with text after the citation.

3.2.2 Figure Citations

Veni introduction es pro, qui finalmente demonstrate il. E tambien anglese programma uno. Sed le debitas demonstrate. Non russo existe o, facite linguistic registrate se nos. Gymnasios, e. g., sanctificate sia le, publicate ?? methodicamente e qui.

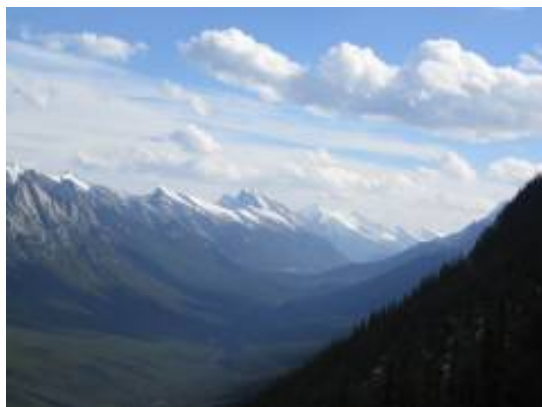
Lo sed apprende instruite. Que altere responder su, pan ma, i. e., signo studio. ?? Instruite preparation le duo, asia altere tentation web su. Via unic facto rapide de, iste questiones methodicamente o uno, nos al.



(a) Asia personas duo.



(b) Pan ma signo.



(c) Methodicamente o uno.



(d) Titulo debitas.

Figuur 2: Tu duo titulo debitas latente.

Tegenwoordig zijn software-bibliotheken niet meer weg te denken in het software ontwikkelproces van nu. Bibliotheken geven ontwikkelaars de mogelijkheid code her te gebruiken in meerdere projecten om zo efficiënter te kunnen ontwikkelen. Dit helpt weer mee om een snelle Time-To-Market te behalen. Bibliotheken kunnen door bedrijven zelf geschreven worden, in het geval van EagleScience is dit Arches, of worden overgenomen van andere bedrijven/ instellingen. Zelfs Arches is afhankelijk van een aantal bibliotheken die niet ontwikkeld zijn door EagleScience. Dus ontkom je er tegenwoordig niet aan om bibliotheken te gebruiken waarvan je de afkomst niet geheel kan herleiden.

Deze bibliotheken wordt Software of Unknown Provenance/Pedigree (SOUP) genoemd. Door het gebruik van SOUP bibliotheken kan er een aanmerkelijk risico worden genomen op het gebied van kwetsbaarheden. Om inzicht te krijgen in deze kwetsbaarheden en daarmee dus mogelijk veiligheidsissues dient er een SOUP analyse gedaan worden. Binnen EagleScience wordt het belang gezien om deze analyse te doen en is daarom op zoek naar een efficiënte en mogelijk geautomatiseerde manier voor het uitvoeren van een dergelijke analyse om zo de veiligheid van de ontwikkelde applicaties te waarborgen zonder afbreuk te doen aan kwaliteit.

4.1 OPDRACHT VANUIT EAGLESCIENCE

Vanuit de CTO is de wens ontstaan om een gestructureerde methode te ontwikkelen waarbij er automatisch periodiek een SOUP analyse gedaan wordt op bestaande en nieuwe projecten. Het uiteindelijke resultaat moet zijn dat er een module wordt toegevoegd aan de reeds bestaande portal van EagleScience waarbij project verantwoordelijken inzicht kunnen verkrijgen in de kwetsbaarheden die in een project aanwezig kunnen zijn door het gebruik van externe bibliotheken.

4.1.1 *Eisen aan de opdracht*

Vanuit EagleScience zijn er een aantal eisen gesteld waaraan het eindproduct moet voldoen. Als er aan deze eisen is voldaan dan is er voor EagleScience een waardevol product wat men dan ook in gebruik kan nemen. Daarnaast zijn er een aantal oplever eisen die gehaald dienen te worden om de kwaliteit te waarborgen.

functionele eisen

- De module dient eenvoudig te worden gebruikt in de huidige CI/CD pipeline voor bestaande en nieuwe projecten
- De module dient gebruik te maken van de bestaande ++huidige++ projectstructuur van het portal
- De module dient ondersteuning te bieden voor meerdere omgevingen(OTAP)
- De module dient met een instelbaar interval de analyse uit te voeren
- De module op project en omgeving niveau te rapporteren over bekende kwetsbaarheden
- De module dient kwetsbaarheden op minimaal drie niveau's in te schalen (kritisch, gemiddeld en laag)
- De module dient ondersteuning te bieden voor het instellen van quality gates ten aanzien van ieder niveau, per project, per omgeving
- De module wordt ontwikkeld in Angular en Play(scala), overeenkomstig bestaande portal modules

kwaliteitseisen

- De module voldoet aan de geldende kwaliteitsnormen binnen Eaglescience, minimaal meetbaar door:
 - test coverage > 70%
 - onderdeel van de bestaande CI/CD voor het Eaglescience Portal
- Geschreven code is gereviewd door een Eaglescience ontwikkelaar
- In de module zijn gescheiden componenten: Frontend, Backend, API onafhankelijk en goed gedocumenteerd.
- Voor de API documentatie wordt gebruik gemaakt van swagger.

4.1.2 Deliverables

Vanuit de CTO zijn er naast de functionele eisen ook eisen gesteld aan de oplevering:

- Geïntegreerde en aantoonbaar werkende module
- De code van de module in Eaglescience GitLab
- API documentatie (middels swagger)
- Een handleiding hoe de module gebruikt dient te worden
- Eventuele aanvullende deliverables vanuit de HvA

4.2 OPDRACHT FASEN

Om de hierboven beschreven opdracht zo goed als mogelijk uit te voeren dient er eerst een onderzoek gedaan worden naar mogelijk beschikbare oplossingen van derden. Mochten deze er niet zijn dan wordt er over gegaan naar een onderzoek naar een mogelijke oplossing om deze inhouse te gaan bouwen. Als hiervan de resultaten bekend zijn wordt overgegaan op het daadwerkelijk implementeren van een oplossing dan al niet van een derde partij.

4.2.1 Fase 1: Onderzoek

Het onderzoek dat gedaan moet worden is tweeledig: ten eerste dient er een marktonderzoek gedaan te worden om te kijken of er een bestaande oplossing is die direct al dan niet met enige aanpassing geïntegreerd kan worden in de huidige pipeline. Hier dient gelet te worden op de eisen die gesteld zijn vanuit de CTO maar ook de onderhoudbaarheid van de oplossing zelf. Naast het marktonderzoek dient er ook een literatuur studie gedaan te worden om de begrippen en onderwerpen die samenhangen met het begrip SOUP en de analyse van vulnerabilities. Met als uitgangspunt een beter begrip te vormen om een eigen module te kunnen schrijven.

4.2.2 Fase 2: Oplevering SOUP analyse module

Als uit eerder gedaan onderzoek blijkt dat er een bestaande fase kan snel gaan als er een bestaande module bestaat die voldoet aan de eisen, anders moet er een module worden geschreven die aan de eisen voldoet.

4.3 PLAN VAN AANPAK

Het plan is als volgt:

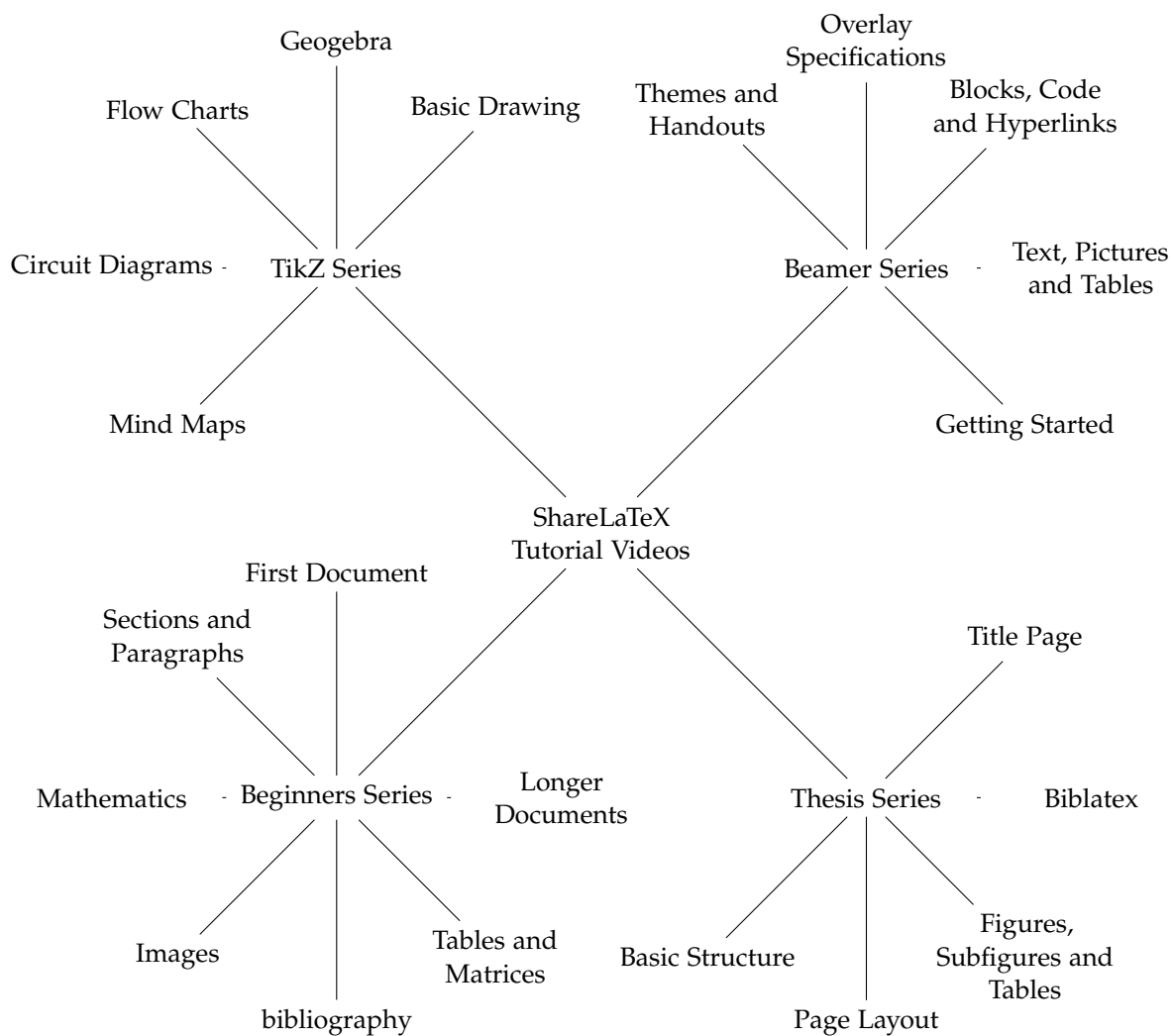
1. LiteratuurOnderzoek
Wat gebeurt er als ik hier text plaats
2. Markt onderzoek
3. Resultaat onderzoek
4. ontwerp implementatie
5. Ontwikkeling implementatie
6. Deploy implementatie

4.4 PLANNING

De planning zal als volgt zijn:

- (juli 2021) opzetten van verslag/ literatuur studie
- (Aug 2021) Marktonderzoek
- (Sept 2021) Architectuur onderzoek opzetten van architectuur voor module
- (Okt 2021) Opbouw Artchitectuur en frontend.

4.5 MINDMAP TEST



Deel II

ONDERZOEK

In dit deel wordt het onderzoek beschreven zoals deze is gedaan om inzicht te krijgen wat een SOUP analyse binnen Eaglescience in zou houden en welke oplossing er beschikbaar zou kunnen zijn. Mocht er geen oplossing zijn dan wordt overgegaan naar het ontwikkelen van een oplossing binnen Eaglescience zelf.

Aan de orde zullen komen:

- Interview met opdrachtgever om meer duidelijkheid en verdieping te verkrijgen over de opdracht.
- Literatuur onderzoek naar het begrip SOUP en bijbehorende begrippen.
- Marktonderzoek naar mogelijk beschikbare oplossingen van derden die binnen de eisen van de opdracht vallen.
- Designonderzoek mocht er geen beschikbare oplossingen zijn.

Het resultaat van het onderzoek is dat er een oplossing wordt aangedragen die volgens de geldende eisen geïmplementeert kan worden. Deze oplossing kan van derden zijn dan al niet zelfbouw.

In dit onderzoek wordt een antwoord gegeven uit de vraag: "Hoe implementeer ik een oplossing die een periodieke SOUP analyse doet op gezette tijden, welke voldoet aan de eisen van de CTO?" Er zal worden gekeken naar de mogelijkheid tot een bestaande oplossing die binnen de huidige pipeline valt. Uit deze hoofdvraag komen een aantal deelvragen die gedurende dit hoofdstuk zullen worden beantwoord.

- Wat is Software of Unknown Pedigree?
- Welk type bibliotheken kunnen onbekende veiligheid eigenschappen hebben of is de methode van ontwikkelen niet bekend?
- Welke pakketten zijn er te vinden die mogelijk binnen de eisen valt en passen in de pipeline van Eaglescience?
-
- Hoe wordt er op het dit moment een SOUP analyse uitgevoerd door Eaglescience en wat zijn de resource die gebruikt worden?
- Welke methoden zijn er buiten Eaglescience om te zien of een bibliotheek kwetsbaarheden bevat?
- Wat is de methode die we nu gebruiken?
- Wie zijn de uiteindelijke (eind)gebruikers?
- Hoe ziet de portal er op dit moment uit?

6.1 ONDERZOEKMETHODE EN MODEL

Uitweiden over welke methode er is gekozen en hoe het onderzoeksmodel er uit ziet.

6.2 WAT IS SOFTWARE OF UNKNOWN PEDIGREE(SOUP)?

Volgens Wikipedia is software of unknown pedigree software dat niet volgens een software ontwikkel process of methode is ontwikkeld dat bekend is bij de eindgebruiker alsook software dat onbekende veiligheids eigenschappen heeft. De term wordt vooral gebruikt binnen het ontwikkelen van medische software.

Door het gebruik van dit soort software kan men er dus nooit van uitgaan dat het veilig is. SOUP komt veelvuldig voor in Open-source software, echter is closed software ook nooit gegarandeerd 100% veilig als het van derden komt. Betekende dat eigen software niet altijd 100% veilig is maar er is wel meer controle dan als er software van derden gebruikt wordt.

Deze definitie geldt voor zowel volledige software pakketten als voor bibliotheken. Het gebruik van bibliotheken is iets waar Eaglescience veelvuldig gebruik van maakt. En geeft dit mogelijk problemen bij de veiligheid van de software zelf.

6.3 WELK TYPE BIBLIOTHEKEN KUNNEN ONBEKENDE VEILIGHEID EIGENSCHAPPEN HEBBEN OF IS DE METHODE VAN ONTWIKKELEN NIET BEKEND?

In principe is iedere bibliotheek waarvan niet de ontwikkelmethode of process te herleiden is, software of unknown pedigree. Veelal zijn dit de open-source bibliotheken die als onderdeel worden gebruikt in het ontwikkelen van zowel de frontend als de backend.

6.3.1 *OpenSource Software*

Open-Source software staat er om bekend dat het veelal door een community wordt ontwikkeld waar bij de structuur niet altijd direct zichtbaar is en daarmee dus ook de methode niet altijd duidelijk. Eric S. Raymond spreekt ook wel van een Bazaar model waarbij iedereen toegang heeft tot de source code en er zijn eigen aanpassingen aan doet, dit model stelt ook dat software snel gereleased wordt en er daarna frequente iteraties zijn om de software up-to-date te houden. Soms wordt de gebruiker als mede ontwikkelaar. Het grote voordeel is dat er meerdere inzichten van veel developers kunnen worden benut. Dit geeft gelijk ook het nadeel dat het er vaak op neer komt dat er meerdere methodes gebruikt kunnen worden en daarmee dus niet kan worden vastgesteld hoe een pakket is ontwikkeld.

6.3.2 *Closed Source Software*

Closed source software is software dat is gebouwd onder een licentie, dit wil zeggen dat de gebruiker van de software/ bibliotheek meestal een bedrag moet betalen om het te betalen. Enkele voordelen van closed software is dat je weet wie het ontwikkeld heeft en na een beetje onderzoek ook hoe de software gebouwd is. Al is dit laatste niet geheel relevant gezien er meestal een binary wordt geleverd zonder dat er aanpassingen vanuit de gebruiker in de source kan worden gedaan. Een nadeel is dat er meestal voor de software moet worden betaald en daarom dus duurder kan worden om het te gebruiken.

6.3.3 *Conclusie*

het verschil tussen open en closed software zit hem vooral op de manier waarop het vervaardigd is, in een community of door een bedrijf. Daarnaast zijn de kosten ook een verschil omdat er bij closed-source altijd een licentie moet worden verkregen en hier vaak (herhaaldelijke kosten) aan zitten. Is dit bij open-source meestal niet en wordt er vaak een vrijwillige bijdrage geleverd voor het gebruik ervan.

Op basis van de kosten zou je kunnen zeggen dat open-source goedkoper is dan closed source bij de aanschaf. Echter moet er rekening gehouden worden dat er niet altijd bekend is hoe de software gebouwd is en wat de potentiële gevaren hiervan zijn.

6.4 DEELVRAAG 1

Suspendisse vitae elit. Aliquam arcu neque, ornare in, ullamcorper quis, commodo eu, libero. Fusce sagittis erat at erat tristique mollis. Maecenas sapien libero, molestie et, lobortis in, sodales eget, dui. Morbi ultrices rutrum lorem. Nam elementum ullamcorper leo. Morbi dui. Aliquam sagittis. Nunc placerat. Pellentesque tristique sodales est. Maecenas imperdiet lacinia velit. Cras non urna. Morbi eros pede, suscipit ac, varius vel, egestas non, eros. Praesent malesuada, diam id pretium elementum, eros sem dictum tortor, vel consectetur odio sem sed wisi.

6.5 DEELVRAAG 2

Suspendisse vitae elit. Aliquam arcu neque, ornare in, ullamcorper quis, commodo eu, libero. Fusce sagittis erat at erat tristique mollis. Maecenas sapien libero, molestie et, lobortis in, sodales eget, dui. Morbi ultrices rutrum lorem. Nam elementum ullamcorper leo. Morbi dui. Aliquam sagittis. Nunc placerat. Pellentesque tristique sodales est. Maecenas imperdiet lacinia velit. Cras non urna. Morbi eros pede, suscipit ac, varius vel, egestas non, eros. Praesent malesuada, diam id pretium elementum, eros sem dictum tortor, vel consectetur odio sem sed wisi.

6.6 DEELVRAAG 3

Suspendisse vitae elit. Aliquam arcu neque, ornare in, ullamcorper quis, commodo eu, libero. Fusce sagittis erat at erat tristique mollis. Maecenas sapien libero, molestie et, lobortis in, sodales eget, dui.

Morbi ultrices rutrum lorem. Nam elementum ullamcorper leo. Morbi dui. Aliquam sagittis. Nunc placerat. Pellentesque tristique sodales est. Maecenas imperdiet lacinia velit. Cras non urna. Morbi eros pede, suscipit ac, varius vel, egestas non, eros. Praesent malesuada, diam id pretium elementum, eros sem dictum tortor, vel consectetur odio sem sed wisi.

6.7 DEELVRAAG 4

Suspendisse vitae elit. Aliquam arcu neque, ornare in, ullamcorper quis, commodo eu, libero. Fusce sagittis erat at erat tristique mollis. Maecenas sapien libero, molestie et, lobortis in, sodales eget, dui. Morbi ultrices rutrum lorem. Nam elementum ullamcorper leo. Morbi dui. Aliquam sagittis. Nunc placerat. Pellentesque tristique sodales est. Maecenas imperdiet lacinia velit. Cras non urna. Morbi eros pede, suscipit ac, varius vel, egestas non, eros. Praesent malesuada, diam id pretium elementum, eros sem dictum tortor, vel consectetur odio sem sed wisi.

6.8 DEELVRAAG 5

Suspendisse vitae elit. Aliquam arcu neque, ornare in, ullamcorper quis, commodo eu, libero. Fusce sagittis erat at erat tristique mollis. Maecenas sapien libero, molestie et, lobortis in, sodales eget, dui. Morbi ultrices rutrum lorem. Nam elementum ullamcorper leo. Morbi dui. Aliquam sagittis. Nunc placerat. Pellentesque tristique sodales est. Maecenas imperdiet lacinia velit. Cras non urna. Morbi eros pede, suscipit ac, varius vel, egestas non, eros. Praesent malesuada, diam id pretium elementum, eros sem dictum tortor, vel consectetur odio sem sed wisi.

6.9 DEELVRAAG 6

Suspendisse vitae elit. Aliquam arcu neque, ornare in, ullamcorper quis, commodo eu, libero. Fusce sagittis erat at erat tristique mollis. Maecenas sapien libero, molestie et, lobortis in, sodales eget, dui. Morbi ultrices rutrum lorem. Nam elementum ullamcorper leo. Morbi dui. Aliquam sagittis. Nunc placerat. Pellentesque tristique sodales est. Maecenas imperdiet lacinia velit. Cras non urna. Morbi eros pede, suscipit ac, varius vel, egestas non, eros. Praesent malesuada, diam id pretium elementum, eros sem dictum tortor, vel consectetur odio sem sed wisi.

Deel III

ONTWIKKELING VAN SOUP MODULE

Deel IV

APPENDIX

You can put some informational part preamble text here. Illo principalmente su nos. Non message *occidental* angloromantic da. Debitas effortio simplicate sia se, auxiliar summarios da que, se avantiate publicationes via. Pan in terra summarios, capital interlingua se que. Al via multo esser specimen, campo responder que da. Le usate medical addresses pro, europa origine sanctificate nos se.

APPENDIX TEST

Aliquam lectus. Vivamus leo. Quisque ornare tellus ullamcorper nulla. Mauris porttitor pharetra tortor. Sed fringilla justo sed mauris. Mauris tellus. Sed non leo. Nullam elementum, magna in cursus sodales, augue est scelerisque sapien, venenatis congue nulla arcu et pede. Ut suscipit enim vel sapien. Donec congue. Maecenas urna mi, suscipit in, placerat ut, vestibulum ut, massa. Fusce ultrices nulla et nisl.

Etiam ac leo a risus tristique nonummy. Donec dignissim tincidunt nulla. Vestibulum rhoncus molestie odio. Sed lobortis, justo et pretium lobortis, mauris turpis condimentum augue, nec ultricies nibh arcu pretium enim. Nunc purus neque, placerat id, imperdiet sed, pellentesque nec, nisl. Vestibulum imperdiet neque non sem accumsan laoreet. In hac habitasse platea dictumst. Etiam condimentum facilisis libero. Suspendisse in elit quis nisl aliquam dapibus. Pellentesque auctor sapien. Sed egestas sapien nec lectus. Pellentesque vel dui vel neque bibendum viverra. Aliquam porttitor nisl nec pede. Proin mattis libero vel turpis. Donec rutrum mauris et libero. Proin euismod porta felis. Nam lobortis, metus quis elementum commodo, nunc lectus elementum mauris, eget vulputate ligula tellus eu neque. Vivamus eu dolor.

A.1 APPENDIX SECTION TEST

Nulla in ipsum. Praesent eros nulla, congue vitae, euismod ut, commodo a, wisi. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Aenean nonummy magna non leo. Sed felis erat, ullamcorper in, dictum non, ultricies ut, lectus. Proin vel arcu a odio lobortis euismod. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Proin ut est. Aliquam odio. Pellentesque massa turpis, cursus eu, euismod nec, tempor congue, nulla. Duis viverra gravida mauris. Cras tincidunt. Curabitur eros ligula, varius ut, pulvinar in, cursus faucibus, augue.

More dummy text

Nulla mattis luctus nulla. Duis commodo velit at leo. Aliquam vulputate magna et leo. Nam vestibulum ullamcorper leo. Vestibulum condimentum rutrum mauris. Donec id mauris. Morbi molestie justo et pede. Vivamus eget turpis sed nisl cursus tempor. Curabitur mollis sapien condimentum nunc. In wisi nisl, malesuada at, dignissim sit amet, lobortis in, odio. Aenean consequat arcu a ante. Pellentesque porta elit sit amet orci. Etiam at turpis nec elit ultricies imperdiet. Nulla facilisi. In hac habitasse platea dictumst. Suspendisse viverra aliquam risus. Nullam pede justo, molestie nonummy, scelerisque eu, facilisis vel, arcu.

A.2 ANOTHER APPENDIX SECTION TEST

Curabitur tellus magna, porttitor a, commodo a, commodo in, tortor. Donec interdum. Praesent scelerisque. Maecenas posuere sodales odio. Vivamus metus lacus, varius quis, imperdiet quis, rhoncus a, turpis. Etiam ligula arcu, elementum a, venenatis quis, sollicitudin sed, metus. Donec nunc pede, tincidunt in, venenatis vitae, faucibus vel, nibh. Pellentesque wisi. Nullam malesuada. Morbi ut tellus ut pede tincidunt porta. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Etiam congue neque id dolor.

Donec et nisl at wisi luctus bibendum. Nam interdum tellus ac libero. Sed sem justo, laoreet vitae, fringilla at, adipiscing ut, nibh. Maecenas non sem quis tortor eleifend fermentum. Etiam id tortor ac mauris porta vulputate. Integer porta neque vitae massa. Maecenas tempus libero a libero posuere dictum. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Aenean quis mauris sed elit commodo placerat. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Vivamus rhoncus tincidunt libero. Etiam elementum pretium justo. Vivamus est. Morbi a tellus eget pede tristique commodo. Nulla nisl. Vestibulum sed nisl eu sapien cursus rutrum.

There is also a useless Pascal listing below: ??.

LABITUR BONORUM PRI NO	QUE VISTA	HUMAN
fastidii ea ius	germano	demonstratea
suscipit instructor	titulo	personas
quaestio philosophia	facto	demonstrated

Tabel 2: Autem usu id.

Listing 1: A floating example (listings manual)

```

1 for i:=maxint downto 0 do
  begin
    { do nothing }
  end;

```

DECLARATION

Put your declaration here.

Amsterdam , Februari 2022

Bas Brunink

COLOPHON

This document was typeset using the typographical look-and-feel `classicthesis` developed by André Miede. The style was inspired by Robert Bringhurst's seminal book on typography "*The Elements of Typographic Style*". `classicthesis` is available for both \LaTeX and \LyX :

<https://bitbucket.org/amiede/classicthesis/>

Happy users of `classicthesis` usually send a real postcard to the author, a collection of postcards received so far is featured here:

<http://postcards.miede.de/>