Project Design Document

Projekt: Global Unified Automated Response and Disaster Intelligence Alert Network (GUARDIAN)

Przedmiot: Zarządzanie projektem informatycznym

Grupa nr: 2

Zespół:

- ***Ruslan Zhukotynskyi - kierownik***
- ***Remigiusz Sęk***
- ***Jakub Pawlak***

Spis treści:

1. Badania podstawowe – I poziom wg skali TLR

a. Idea

W związku z narastającym problemem, jakim jest globalne ocieplenie, ludzkość mierzy się z rosnącymi w siłę klęskami żywiołowymi. Nie jest tajemnicą, że temperatura na naszej planecie z roku na rok rośnie, co w końcowym rozrachunku może doprowadzić do przytłaczającej liczby kataklizmów. Do rozwiązania tego problemu można wykorzystać potencjał danych wytwarzanych przez sensory z różnych części ziemi, mogłaby to być dobra okazja do usprawnienia synchronizacji i integracji między istniejącymi już lokalnymi systemami takimi jak np. satelity czy systemy wykrywania trzęsień ziemi. Być może w ten sposób udałoby się lepiej informować i instruować mieszkańców zagrożonych terenów lub poprawić współpracę między organami państwowymi. Taki projekt mógłby też pomóc z utworzeniem odpowiednich fortyfikacji przed nadciągającymi klęskami żywiołowymi.

2. Badania przemysłowe – II poziom wg skali TLR

a. Koncepcja technologii

Przeprowadzono wstępną analizę możliwości technologicznych związanych z integracją danych o klęskach żywiołowych na terenie Polski. Ustalono, że optymalnym rozwiązaniem jest stworzenie systemu opartego na architekturze API, który będzie integrował dane w czasie rzeczywistym z różnych źródeł, takich jak IMGW, EUMETSAT, NASA FIRMS, Copernicus czy EMSC. Opracowywany system ma działać jako warstwa pośrednia, która będzie interpretować wyniki z zewnętrznych interfejsów, przetwarzać je i udostępniać w zunifikowanym formacie dla innych aplikacji i systemów ostrzegania.

W ramach koncepcji zaprojektowano, aby system analizował dane w czasie rzeczywistym dotyczące m.in. powodzi, pożarów, burz, sztormów oraz trzęsień ziemi, a następnie na ich podstawie generował odpowiednie komunikaty ostrzegawcze. Mechanizm ten może być zintegrowany z lokalnymi kanałami powiadamiania, takimi jak SMS, e-mail, aplikacje mobilne czy systemy miejskie, umożliwiając szybkie i automatyczne informowanie mieszkańców zagrożonych obszarów.

Zastosowanie takiej technologii w przyszłości pozwoliłoby zwiększyć skuteczność działań prewencyjnych i operacyjnych służb ratunkowych, usprawnić wymianę informacji między instytucjami państwowymi oraz poprawić ogólny poziom bezpieczeństwa obywateli.

b. Lista rzeczy

i. API

1. NASA FIRMS (do pożarów)
2. EMSC Real-time Feed (do trzęsień ziemi),
3. Copernicus GFM (Sentinel-1) (do powodzi)
4. EUMETSAT Meteosat RSS (do burz/wichur)
5. Copernicus CDS (ERA5-Land) (do upałów/susz)
6. Copernicus Marine (CMEMS) (do sztormów morskich)

ii. Inne

1. 6-10 komputerów stacjonarnych o wysokiej mocy obliczeniowej (z kartami GPU) tak aby było można trenować modele sztucznej inteligencji oraz przetwarzać duże zbiory danych,
2. serwer do obsługi API i integracji danych
3. środowisko testowe,
4. środowisko chmurowe,
5. dostęp światłowodowy do Internetu,
6. system zarządzania bazami danych
7. środowisko programistyczne i analityczne na każdym komputerze + github i ERP (Python, TensorFlow, PyTorch, FastAPI, Docker, Visual Studio Code, GitHub / GitLab, Jira / Trello)

3. Badania przemysłowe – III poziom wg skali TLR

W ramach III poziomu gotowości technologicznej systemu GUARDIAN zostaną przeprowadzone prace badawcze oraz potwierdzenie słuszności założenia koncepcji.

a. Moduł integracji

System **zbiera** dane ze wszystkich wybranych źródeł API w sposób **niezależny siebie**, następnie **normalizuje** otrzymane dane do jednolitej postaci w celu prostszej interpretacji. Zbiera te dane i **wysyła** do innego modułu w znormalizowanej formie.

b. Moduł interpretacji AI

Po otrzymaniu znormalizowanych danych z modułu integracji, AI **interpretuje** wyniki i **tworzy** wytyczne dla odpowiednich służb odnośnie zalecanych poczynań oraz wyposażenia. W ramach tego etapu opracowany zostanie wstępny model AI, który zostanie wytrenowany z wykorzystaniem przygotowanych zbiorów danych symulacyjnych oraz dostępnych archiwalnych danych środowiskowych pochodzących z publicznych źródeł. Model ten będzie miał za zadanie poprawnie analizować przekazane dane wejściowe, identyfikować wzorce charakterystyczne dla poszczególnych zjawisk oraz generować komunikaty i zalecenia operacyjne dla służb.

c. Moduł sugestii służb

Na podstawie interpretacji AI **oceniane** jest ryzyko katastrofy i **szacowane** są potrzebne zasoby do rozwiązania sytuacji. Gdy zasoby są już oszacowane **poszukiwane** są odpowiednie służby w podanej ilości, następnie jest sprawdzane wyposażenie danych służb, jeżeli spełniają kryteria to dane są przekazywane do modułu wysyłki, jeżeli nie to szuka się dalej aż zostaną spełnione wymogi AI.

d. Moduł sprawdzenia wyposażenia

Każda służba musi prowadzić **monitoring** stanu wyposażenia oraz zasobów ludzkich dla informacji ogólnej na podstawie której można szybko przesyłać informacje zwrotne do systemu bez opóźnień w czasie rzeczywistym.

e. Moduł informowania służb

Zalecenia otrzymane przez AI zostają **rozesłane** do odpowiednich służb, z informacjami takimi jak zalecane wyposażenie, miejsce zjawiska, **zalecanymi** działaniami oraz **siłą** kataklizmu.

f. Moduł informowania obywateli

Rozesłane zostaną na numery telefonów obywateli zagrożonego obszaru odpowiednie informacje. Numery telefonów i adresy urządzeń docelowych są wybierane na podstawie geolokalizacji oraz danych administracyjnych z rejestrów mieszkańców lub lokalnych baz danych.

4. Badania przemysłowe – IV poziom wg skali TLR

a. Weryfikacja koncepcji w warunkach laboratoryjnych

i. Moduł integracji

Pobrano dane z różnych API z losowo wybranych 50 miejsc z Polski. Moduł integracji przetwarzał początkowo dane bez dodatkowych poprawek, co ujawniło błędy w normalizacji, takie jak różne jednostki miar temperatury, niejednolite znaczniki czasu, brakujące pola oraz różny sposób określania lokalizacji – w niektórych przypadkach obszar katastrofy był podany jako współrzędne punktowe, a w innych jako szerszy region administracyjny.

Po wprowadzeniu funkcji korekcji i standaryzacji danych, w tym konwersji jednostek, ujednolicenia formatu daty, walidacji pól obowiązkowych oraz normalizacji sposobu zapisu lokalizacji, moduł poprawnie znormalizował wszystkie rekordy i przesyła je dalej do modułu interpretacji AI.

ii. Moduł interpretacji AI

Przygotowano zestaw kontrolny 200 przypadków symulacyjnych obejmujących pożary, powodzie, burze i trzęsienia ziemi z wykorzystaniem danych archiwalnych wykonano 100 serii testów weryfikujących poprawność analizy danych wejściowych, identyfikacji wzorów zjawisk oraz generowania komunikatów operacyjnych.

Model wykazał odchylenia w rozpoznawaniu intensywności burz - blednie klasyfikował 15% przypadków. Ustalono, że na wynik ma wpływ niedostateczna reprezentacja danych o burzach w zbiorze treningowym. Uzupełniono zbiór o 50 dodatkowych przypadków i przeprowadzono trening na nowo. Po ponownych testach

dokładność klasyfikacji wzrosła do 94% a generowane zalecenia były zgodne z procedurami operacyjnymi służb.

iii. Moduł sugestii służb

Przygotowano zestaw kontrolny 80 scenariuszy katastroficznych z różnymi poziomami ryzyka. Wykonano 80 serii testów weryfikujących poprawność oszacowania zasobów, doboru służb według kryteriów oraz walidacji wyposażenia.

Moduł wykazał opóźnienia w wyszukiwaniu służb dla scenariuszy wymagających więcej niż 5 typów jednostek jednocześnie. Ustalono, że na wynik ma wpływ nieoptymalne zapytanie do bazy danych służb. Zoptymalizowano algorytm wyszukiwania i ponownie wykonano testy. Czas doboru służb skrócił się o 60%, a wszystkie scenariusze zostały obsłużone zgodnie z wymogami AI.

iv. Moduł sprawdzenia wyposażenia

Przygotowano zestaw kontrolny 30 jednostek służb ratunkowych zróżnicowanych pod względem stanu wyposażenia, liczby personelu oraz dostępności pojazdów. Wykonano 150 serii testów weryfikujących kompletność danych, poprawność mapowania pól oraz aktualność raportów przesyłanych w czasie rzeczywistym. W trakcie testów zidentyfikowano niespójność danych pomiędzy jednostkami. W 7 przypadkach raporty zawierały nieaktualne informacje o liczbie dostępnych pojazdów lub błędne oznaczenia typów sprzętu. Ustalono, że przyczyną był brak walidacji schematu danych oraz różnice w formacie raportowania pomiędzy jednostkami.

Wprowadzono jednolity schemat raportowania, ujednolicono nazewnictwo pól oraz dodano automatyczną walidację kompletności rekordów. Po ponownym wykonaniu 150 serii testów wszystkie dane były aktualizowane w czasie poniżej 10 sekund, a spójność i kompletność rekordów osiągnęły poziom 98%.

v. Moduł informowania służb

Przygotowano zestaw kontrolny 60 komunikatów dla różnych typów służb i poziomów zagrożenia. Wykonano 60 serii testów weryfikujących kompletność przekazanych informacji (wyposażenie, lokalizacja, działania, intensywność) oraz czas dostarczenia.

Moduł wykazał brakujące dane o sile kataklizmu w 20% komunikatów dla zdarzeń o średnim ryzyku. Ustalono, że na wynik ma wpływ nieprawidłowe mapowanie danych z modułu interpretacji AI. Poprawiono schemat integracji danych i ponownie wykonano testy. Wszystkie komunikaty zawierały kompletne informacje i były dostarczane w czasie do 5 sekund.

vi. Moduł informowania obywateli

Przygotowano zestaw kontrolny 500 numerów testowych rozlokowanych w 10 różnych strefach geograficznych. Wykonano 100 serii testów weryfikujących poprawność

selekcji numerów na podstawie geolokalizacji, treść komunikatów oraz pokrycie zagrożonego obszaru.

Moduł wykazał pominięcie 12% numerów w strefach granicznych między dwoma obszarami administracyjnymi. Ustalono, że na wynik ma wpływ precyzyjny algorytm określenia przynależności do strefy. Zmodyfikowano logikę geolokalizacji z uwzględnieniem buforów granicznych i ponownie wykonano testy. Pokrycie obszaru wzrosło do 99.5% a wszystkie komunikaty zostały dostarczone w ciągu 30 sekund.

b. Określone ryzyka

i. Ryzyko 1

Istnieje ryzyko otrzymania błędnych lub niepełnych danych z jednego z zewnętrznych API. Może się to zdarzyć w wyniku awarii serwisu lub chwilowego braku połączenia. W takiej sytuacji system GUARDIAN może błędnie ocenić sytuację zagrożenia lub pominąć niektóre zdarzenia, co zmniejsza skuteczność jego działania.

Rozwiązanie: Aby ograniczyć to ryzyko, system zostanie wyposażony w mechanizm automatycznej weryfikacji danych pochodzących z różnych źródeł. Jeśli jedno API przestanie działać lub zwróci dane o podejrzanej strukturze, moduł integracji automatycznie wykorzysta alternatywne źródła (Copernicus EMSR Hotspots, GFZ GEOFON Earthquake Bulletin, Copernicus EMS Rapid Mapping, NOAA GOES Real-Time Imagery, NOAA NCEP Climate Data, NOAA WaveWatch III) lub dane historyczne. Dodatkowo przewidziana jest możliwość automatycznego raportowania błędów do zespołu technicznego oraz bezpośredniego kontaktu z dostawcami danych, aby możliwe było szybkie usunięcie przyczyny problemu.

ii. Ryzyko 2

Opóźnienia w czasie rzeczywistym przy synchronizacji danych z wielu źródeł API.

Rozwiązanie: Zastosowanie asynchronicznego pobierania danych z kolejkami priorytetowymi i mechanizmem cache'owania dla danych o niskiej zmienności.

iii. Ryzyko 3

Istnieje ryzyko, że dane dotyczące wyposażenia i zasobów służb ratowniczych w module sprawdzenia wyposażenia mogą być nieaktualne. Może to prowadzić do sytuacji, w której system przydzieli jednostkę, która w danym momencie nie dysponuje wymaganym sprzętem lub personelem, co obniża skuteczność akcji ratowniczej.

Rozwiązanie: W celu wyeliminowania tego ryzyka zostanie wdrożony system tzw. heartbeat monitoring, który będzie cyklicznie sprawdzał i potwierdzał aktualność danych przekazywanych przez poszczególne jednostki. Dodatkowo przed przydzieleniem zadania system automatycznie przeprowadzi zapytanie weryfikujące stan sprzętu i gotowość operacyjną służb, aby mieć pewność, że informacje są aktualne i wiarygodne.

5. Grupa docelowa

Grupa docelowa - w skład grupy docelowej wchodzą jednostki i instytucje odpowiedzialne za zarządzanie bezpieczeństwem publicznym, reagowanie kryzysowe oraz monitorowanie zagrożeń. Do takich podmiotów wchodzą wszelkie wojewódzkie centra zarządzania kryzysowe które będą w stanie na duży obszar wykorzystać zdolność detekcji i koordynacji akcji. Na nieco mniejszą skalę powiaty.

Model biznesowy (sprzedażowy) - System będzie sprzedawany dla podmiotów z umową na 5 lat użytkowania z wpłatą początkową i rozliczaniem comiesięcznym w formie maintenance. Oznacza to podpisanie zobowiązania wieloletniego, w którym klient otrzymuje gwarancję dostępu do platformy, regularne aktualizacje funkcji i modeli AI, wsparcie techniczne oraz pakiet szkoleń i testów interoperacyjnych przez cały okres obowiązywania umowy.

6. Weryfikacja koncepcji w środowisku zbliżonym do rzeczywistego

W celu połączenia poszczególnych modułów systemu, zastosowano architekturę mikroserwisową, w której każdy moduł funkcjonuje jako niezależny serwis komunikujący się z pozostałymi za pośrednictwem centralnego Orchestratora systemu. Orchestrator odpowiada za koordynację przepływu danych, kontrolę spójności komunikacji, reagowanie na błędy transmisji oraz monitorowanie statusu poszczególnych mikroserwisów. Wszystkie moduły wymieniają dane poprzez zdefiniowane interfejsy REST API, z zastosowaniem formatu JSON oraz protokołu HTTPS.

W środowisku testowym przeprowadzono pełny cykl wymiany danych między modułami – od pobrania danych z zewnętrznych API (moduł integracji), przez ich analizę przez moduł interpretacji AI, dobór służb i sprawdzenie wyposażenia, aż po generację komunikatów dla służb i obywateli. W ramach testu wykorzystano dane pochodzące z 50 lokalizacji z Polski oraz dane custom eksperymentalne, obejmujące różne typy zjawisk środowiskowych (pożary, powodzie, burze).

6.1 Moduł integracji API

Dokonano integracji modułu z centralnym Orchestratorem systemu. Przeprowadzono testy poprawności pobierania danych z zewnętrznych API, obejmujących różne źródła danych środowiskowych. Test wykonano na próbnej bazie obejmującej 50 lokalizacji z terenu Polski. Weryfikowano poprawność normalizacji danych, konwersję jednostek, ujednolicenie formatów daty oraz kompletność pól. Zidentyfikowano przypadki błędnej interpretacji formatu lokalizacji (współrzędne vs. region administracyjny), które mogły prowadzić do błędnego przypisania zdarzeń. Wprowadzone poprawki obejmowały ujednolicenie schematu danych wejściowych oraz automatyczną walidację struktur JSON. Po ponownym teście wszystkie rekordy zostały poprawnie przetworzone i przesłane do modułu interpretacji AI.

6.2 Moduł interpretacji AI

Zintegrowano moduł z centralnym Orchestratorem i modułem integracji. Przeprowadzono testy analityczne na 600 przypadkach symulacyjnych obejmujących różne typy zjawisk. Weryfikowano skuteczność klasyfikacji zdarzeń, dokładność oceny intensywności oraz zgodność generowanych

komunikatów z obowiązującymi procedurami reagowania służb ratunkowych. W trakcie testów odnotowano błędną klasyfikację w 15% przypadków powodziowych, co wynikało z ograniczonej liczby reprezentatywnych danych tego typu w zbiorze treningowym. Dokonano rozszerzenia zbioru treningowego o 66 nowych przypadków i powtórzono proces uczenia modelu. Po ponownej walidacji skuteczność analizy wzrosła do 94%, a wszystkie komunikaty generowane przez moduł były zgodne z danymi wejściowymi.

6.3 Moduł sugestii służb

Dokonano integracji modułu z centralnym Orchestratorem systemu poprzez interfejsy REST API z wykorzystaniem formatu JSON i protokołu HTTPS. Przygotowano zestaw kontrolny 80 scenariuszy katastroficznych o zróżnicowanych poziomach ryzyka. Wykonano 80 serii testów weryfikujących poprawność oszacowania zasobów, doboru służb oraz walidacji wyposażenia. Zidentyfikowano opóźnienia dla scenariuszy wymagających więcej niż 5 typów jednostek, spowodowane nie optymalnymi zapytaniami do bazy danych. Po optymalizacji algorytmu wyszukiwania czas doboru służb skrócił się o 60%, a wszystkie scenariusze zostały obsłużone zgodnie z wymogami systemu.

6.4 Moduł sprawdzenia wyposażenia

Dokonano integracji modułu z Orchestratorem poprzez interfejsy REST API. Przygotowano zestaw kontrolny 30 jednostek służb ratunkowych. Wprowadzono podział raportów na rodzaje sprawdzanych czynności: stan wyposażenia technicznego, dostępność personelu, status pojazdów oraz aktualność certyfikatów, co zwiększyło granularność weryfikacji. Wykonano 150 serii testów weryfikujących kompletność danych i poprawność mapowania pól. W 7 przypadkach zidentyfikowano niespójności spowodowane brakiem walidacji schematu oraz różnicami w formacie raportowania. Po wprowadzeniu jednolitego schematu i automatycznej walidacji dane aktualizowano w czasie poniżej 10 sekund, osiągając 98% spójność rekordów.

6.5 Moduł informowania służb

Dokonano integracji modułu informowania służb z centralnym Orchestratorem systemu. Przeprowadzono testy poprawności przesyłania komunikatów do jednostek ratunkowych oraz centrów zarządzania kryzysowego przy użyciu symulowanego środowiska API. Testy obejmowały 60 scenariuszy katastroficznych dotyczących różnych typów zagrożeń(pożary, powodzie, burze, trzęsienia ziemi). Weryfikowano kompletność przekazywanych danych (lokalizacja, intensywność zjawiska, rekomendowane działania i wyposażenie), czas dostarczenia komunikatu oraz poprawność potwierdzeń odbioru. Zidentyfikowano pojedyncze przypadki błędnych certyfikatów uwierzytelniających, które spowodowały odrzucenie żądania przez serwer odbiorcy. Po ponownej konfiguracji certyfikatów i aktualizacji schematu integracji komunikaty były poprawnie przekazywane do wszystkich odbiorców a średni czas dostarczenia wynosi poniżej 5 sekund.

6.6 Moduł informowania obywateli

Dokonano integracji modułu informowania obywateli z centralnym orchestratorem systemu. Przeprowadzono testy poprawności wysyłki komunikatów ostrzegawczych do obywateli na podstawie danych geolokalizacyjnych w środowisku testowym obejmującym 10 stref geograficznych. Test wykonano z wykorzystaniem symulowanego dostawcy usług SMS i e-mail dla 5000 numerów testowych. Weryfikowano poprawność selekcji odbiorców, kompletność i czytelność treści komunikatów oraz czas ich dostarczenia.

Zidentyfikowano przypadki nieprawidłowego przypisania numerów w strefach granicznych między obszarami administracyjnymi co skutkowało pominięciem części odbiorców. Po wprowadzeniu mechanizmu buforowania stref i ponownym teście wszystkie komunikaty zostały poprawnie dostarczone do właściwych adresatów w czasie poniżej 30 sekund.

7. Analiza SWOT

	Pozytywne	**Negatywne**
Czynniki wewnętrzne	1. Równoległe informowanie służb i obywateli - zmniejsza czas reakcji ludzi na kataklizmy (80%). 2. Elastyczność systemu – łatwa możliwość integracji z nowymi źródłami danych API do kataklizmów (75%). 3. Architektura mikroserwisowa - każdy moduł może być rozwijany niezależnie (95%).	1. Zależność od zewnętrznych API - Wrażliwość na zmiany formatów danych lub czasowe przerwy w dostępie do usług (20%). 2. Złożoność integracji modułów - wymaga dokładnej synchronizacji komunikacji między mikroserwisami i kontroli spójności danych (20%). 3. Krytyczna zależność od dokładności i terminowości danych wprowadzanych przez służby (30%).
Czynniki zewnętrzne	1. Możliwość integracji z krajowymi systemami bezpieczeństwa (70%) 2. W przypadku poprawy sprzętu wykrywającego kataklizmy, np. satelity, może zwiększyć się wydajność naszego systemu.(5%) 3. Finansowanie z podmiotów wyższych (np. UE)(10%) 4. Rozwój krajowej infrastruktury danych i API środowiskowych, co zwiększy dostępność i dokładność danych wykorzystywanych przez system. (55%)	1. Ryzyko ze strony RODO - potencjalna konieczność redukcji danych osobowych (15%). 2. Zagrożenie ze strony cyberprzestępców, w przypadku przejęcia systemu dane mogą wyciec lub zostać zmanipulowane (5%). 3. Zagrożenia ze strony braku regulacji produktów związanych z AI (15%).

S1: Wysoka skuteczność – mechanizm powiadamiania realnie przyspiesza reakcję służb i obywateli.
S2: System łatwo dostosowuje się do nowych źródeł danych i technologii.
S3: Bardzo wysokie prawdopodobieństwo utrzymania – architektura umożliwia szybkie skalowanie i modernizację.

W1: Niska odporność na błędy – awaria lub zmiana formatu danych może czasowo unieruchomić system.
W2: Wysokie wymagania techniczne – trudność w utrzymaniu spójnej komunikacji między mikroserwisami.
W3: Ryzyko opóźnień – błędne lub opóźnione raporty ograniczają skuteczność działania systemu.

O1: Istnieje duże prawdopodobieństwo (około 70%), że projekt zostanie zintegrowany z systemami krajowymi, ponieważ w Polsce rozwijane są inicjatywy cyfryzacji i centralizacji danych o bezpieczeństwie. Wysoki poziom współpracy z instytucjami publicznymi może znacząco zwiększyć funkcjonalność i wiarygodność systemu.
O2: Jest to szansa o niskim prawdopodobieństwie wystąpienia w krótkim czasie, ponieważ rozwój technologii satelitarnych zależy od czynników zewnętrznych. Jednak w perspektywie kilku lat takie ulepszenia mogą znacząco zwiększyć dokładność danych wejściowych i umożliwić bardziej precyzyjne analizy w systemie.
O3: Istnieją programy wspierające rozwój technologii bezpieczeństwa publicznego, jednak proces aplikacji i konkurencja są wymagające.
O4: Szansa średnia, lecz realna. W Polsce trwa proces tworzenia publicznych oraz prywatnych API , oraz tworzenie jednolitych standardów wymiany informacji (API). Jeśli te zmiany będą kontynuowane, system zyska łatwiejszy dostęp do danych w czasie rzeczywistym i poprawia dokładność analiz.

T1: Możliwe ograniczenia w zakresie przetwarzania i przechowywania danych lokalizacyjnych obywateli mogą wymusić modyfikację architektury systemu lub anonimizację informacji, co wpłynie na dokładność powiadomień.
T2: System operujący danymi o infrastrukturze i działaniach służb może stać się celem ataków. Konieczne jest wdrożenie stałych audytów bezpieczeństwa i szyfrowania komunikacji między modułami.
T3: Brak jednoznacznych przepisów dotyczących odpowiedzialności za decyzje systemów wspomaganych AI może powodować trudności w certyfikacji i wdrożeniu rozwiązania na poziomie instytucjonalnym.

8. Badania przemysłowe – VI poziom wg skali TLR

8.1 Model prototypu w warunkach zbliżonych do rzeczywistych

Przeprowadzono pełną integrację wszystkich sześciu modułów systemu GUARDIAN z centralnym Orchestratorem w środowisku testowym odwzorowującym rzeczywiste warunki operacyjne. Aplikacja została przygotowana do zaawansowanych testów w warunkach zbliżonych do rzeczywistych pod kątem: wydajności działania serwerów, jakości i terminowości przekazywanych komunikatów, stabilności działania oraz spójności przepływu danych pomiędzy modułami.Zostanie również przeprowadzony **test użyteczności (usability testing)** dla interfejsu operatorów podmiotów administracyjnych (np. powiatów, województw), którzy będą odpowiedzialni za obsługę systemu i koordynację działań służb.

Testy zostaną podzielone na dwie grupy: **testy serwerowe** i **testy użytkowe**.

Testy serwerowe będą polegały na symulowaniu maksymalnego obciążenia odpowiadającego obsłudze **25 000 równoczesnych zdarzeń alarmowych**, obejmujących zarówno wysyłkę powiadomień do służb, jak i komunikatów SMS do obywateli. System zostanie uruchomiony w trybie ciągłym przez okres **10 dni bez przerw**, a wszystkie dane kontrolne będą rejestrowane w równych interwałach czasowych.
W trakcie testów zostanie sprawdzone, czy moc obliczeniowa serwerów i konfiguracja mikroserwisów są wystarczające do utrzymania wydajności oraz czy:

1. dane przekazywane z modułów analizy są kompletne i spójne,

2. komunikaty alarmowe docierają do obywateli w czasie nieprzekraczającym **30 sekund**,

3. system zachowuje stabilność przy zmiennych warunkach sieciowych oraz podczas awarii poszczególnych węzłów.

Testy użytkowe zostaną przeprowadzone z udziałem dwóch grup: operatorów administracyjnych i służb ratowniczych.

Operatorzy (np. przedstawiciele jednostek samorządowych lub centralnych) będą korzystać z **interfejsu operatorskiego**, umożliwiającego podgląd zdarzeń, lokalizację zagrożeń, przekazywanie informacji do służb oraz odbieranie raportów o stanie wyposażenia jednostek terenowych.

Służby otrzymają natomiast automatyczne powiadomienia z systemu, zawierające **informacje o lokalizacji zdarzenia, rodzaju zagrożenia, składzie jednostek reagujących** oraz **sugestię sprzętu i zasobów**, które powinny zostać przygotowane.

W testach przewidziano udział **50 operatorów** i **100 przedstawicieli służb**, którzy przeprowadzą symulowane procedury zgłoszenia i reakcji. Oceniana będzie poprawność przepływu informacji, terminowość dostarczania powiadomień oraz spójność danych o stanie gotowości jednostek.

Równolegle przeprowadzone zostaną testy **dystrybucji komunikatów SMS i e-mail** do grupy **500 obywateli**. Weryfikowany będzie czas dostarczenia komunikatu, jego poprawność geolokalizacyjna oraz czytelność treści.

Wyniki testów umożliwią ocenę skuteczności działania modułów komunikacyjnych oraz potwierdzą możliwość wykorzystania systemu w rzeczywistych scenariuszach kryzysowych.
Ewentualne problemy wykryte podczas testów – takie jak błędne przypisania lokalizacji, opóźnienia w transmisji danych lub nieczytelne treści komunikatów – zostaną zidentyfikowane i skorygowane w kolejnym etapie rozwoju (TRL 7).

W efekcie realizacji VI poziomu gotowości technologicznej powstanie **w pełni zintegrowany, przetestowany w warunkach operacyjnych prototyp systemu GUARDIAN**, umożliwiający efektywne informowanie służb i obywateli o zagrożeniach w czasie rzeczywistym. Uzyskane wyniki oraz opinie użytkowników posłużą do dalszej optymalizacji systemu i jego wdrożenia pilotażowego w środowisku administracyjnym.

8.2 Ryzyka technologiczne, które mogą powstać

Ryzyko 1:
Opis: Możliwe przeciążenie Orchestratora przy równoczesnym napływie 25 000 zdarzeń alarmowych, co może powodować opóźnienia w przekazywaniu komunikatów.
Rozwiązanie: Wprowadzenie mechanizmów kolejkowania zadań (queue management) oraz skalowanie poziome mikroserwisów, aby równomiernie rozłożyć obciążenie.

Ryzyko 2:
Opis: Opóźnienia w dostarczaniu powiadomień SMS do obywateli w przypadku awarii sieci lub przeciążenia kanałów komunikacyjnych.
Rozwiązanie: Wprowadzenie redundantnych kanałów transmisji i monitoringu czasu dostarczenia powiadomień, aby zapewnić przekazywanie informacji alternatywnymi ścieżkami.

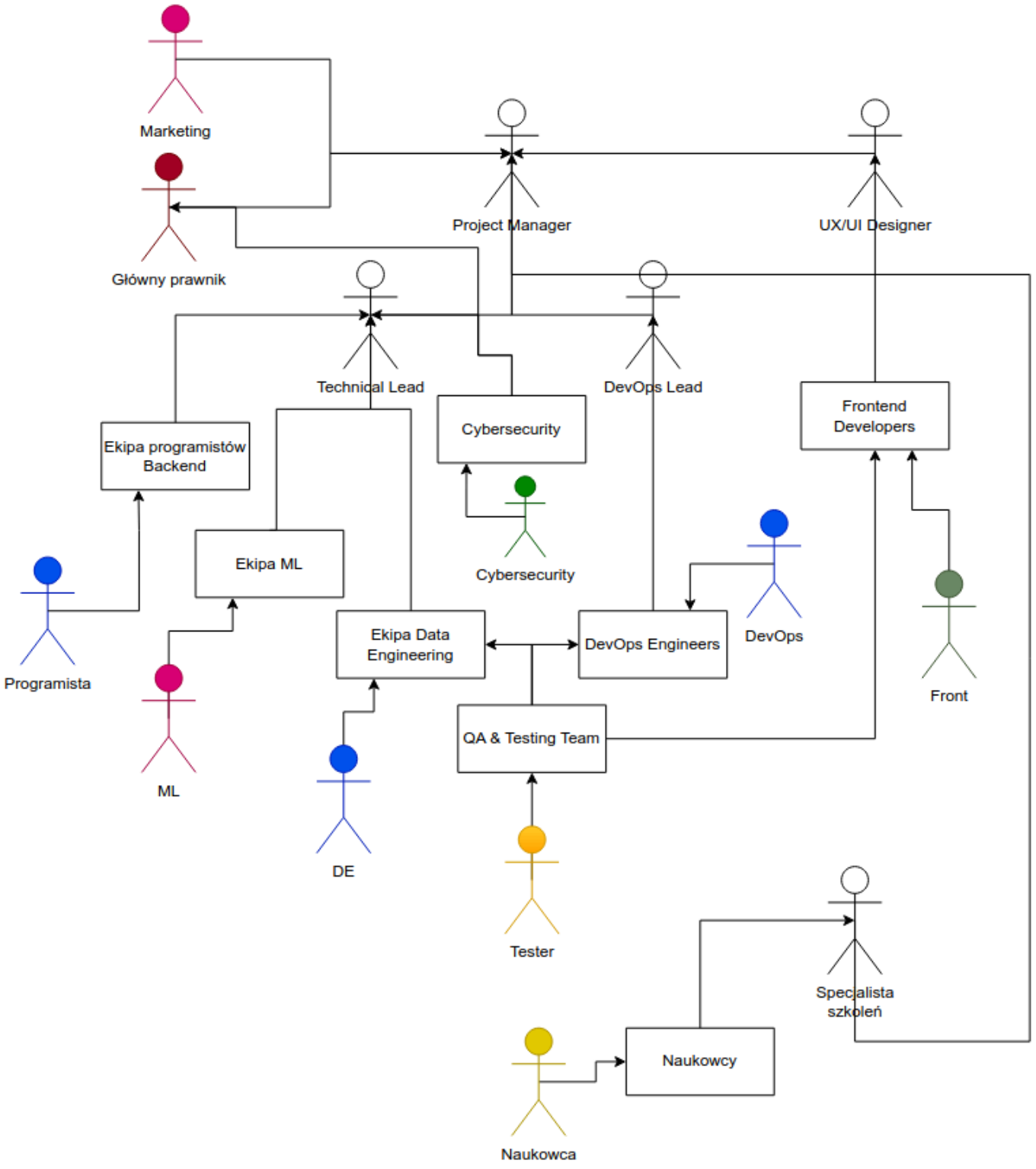
Ryzyko 3:
Opis: W przypadku jednoczesnego wystąpienia wielu zdarzeń w bliskiej lokalizacji system może przypisać nieoptymalnie służby ratunkowe – np. przydzielić jedną służbę do każdego punktu, ignorując możliwość skoordynowanego działania jednej jednostki na kilku punktach lub priorytetyzacji interwencji. Może to prowadzić do sytuacji, w której część zdarzeń nie zostanie obsłużona efektywnie, a zasoby zostaną rozproszone nieoptymalnie.
Rozwiązanie: Wprowadzenie algorytmu priorytetyzacji i grupowania zdarzeń w obrębie jednej strefy geograficznej, tak aby przypisywanie służb uwzględniało rzeczywiste możliwości interwencji i dostępność jednostek. Można też zastosować mechanizm dynamicznego przydzielania zasobów w oparciu o symulację czasu dotarcia oraz intensywności zdarzeń, tak aby jedna jednostka mogła obsłużyć kilka punktów, jeśli jest to możliwe, a nadmiarowe jednostki nie były wysyłane tam, gdzie nie są potrzebne.

9. Zarządzanie jakością i struktura organizacyjna projektu

9.1 Metryka produktu

Metryka produktu: System wczesnego ostrzegania GUARDIAN		
Czas generowania alertu od wykrycia zdarzenia	7 sekund	Średni czas od detekcji kataklizmu do wysłania alertu
Czas dostarczenia SMS do obywatela	30 sekund	Pomiar z systemu SMS gateway
Skuteczność dostarczenia alertów	99%	Procent skutecznie dostarczonych wiadomości
Czas reakcji interfejsu operatorskiego	5 sekund	Średni czas ładowania i reakcji GUI dla operatora
Dokładność klasyfikacji zdarzeń AI	94%	Test na zbiorze kontrolnym zdarzeń
Stabilność systemu pod obciążeniem (25 000)	Bez błędów krytycznych	Test obciążenia przez 10 dni
Czas aktualizacji statusu służb	60 sekund	Synchronizacja danych ze służbami
Czas pobierania danych z API	5 sekund	Czas zbierania informacji z API

9.2 Diagram struktury organizacji projektu



9.3 Role

9.3.1 Project Manager

Project Manager odpowiada za całokształt realizacji projektu: harmonogram, budżet, zasoby, ryzyka i komunikację z kluczowymi interesariuszami (zamawiający, urzędy, partnerzy). Pełni funkcję koordynacyjną między zespołami technicznymi i biznesowymi, prowadzi cotygodniowe spotkania statusowe, przygotowuje raporty i decyzje projektowe. Zaangażowanie: 100% (full-time) — to najintensywniejsza rola; ok. 40–50% czasu na zarządzanie projektem operacyjnym, 30% na kontakty z interesariuszami, reszta na zarządzanie

ryzykiem i dokumentację. Cały czas pilnuje pracę innych uczestników projektu oraz stara się powiązać prace z różnych zespołów tak żeby w wyniku projekt był spójny i każdy element systemu był powiązany.

9.3.2 Technical Lead

Odpowiada za projekt architektury systemu (mikroserwisy, orchestrator, wzorce integracji, bezpieczeństwo) oraz za decyzje technologiczne. Nadzoruje review architektury, pomaga zespołom backend i ML w implementacji wzorców i modeli. Zaangażowanie: **100%** w fazie projektowania i wdrożenia; potem **50–70%** jako nadzór i wsparcie krytycznych zmian.

9.3.3 DevOps Lead

DevOps Lead odpowiada za całą infrastrukturę techniczną projektu — CI/CD, kontenery, Kubernetes, środowiska testowe i produkcyjne. Projektuje procesy wdrażania, automatyzuje deploymenty oraz monitoruje system pod kątem awarii i obciążenia 25 000 zdarzeń. Wspiera zespoły developerskie w konfiguracji środowisk i odpowiada za zgodność z zasadami bezpieczeństwa. Jego praca jest intensywna zwłaszcza w fazach testów, wdrożeń i integracji nowych modułów.

9.3.4 UI/UX Designer

UI/UX Designer projektuje interfejs operacyjny dla podmiotów. Tworzy makiety, prototypy i przeprowadza testy użyteczności, zapewniając czytelność i intuicyjność systemu w sytuacjach kryzysowych. Współpracuje z operatorami oraz testerami użyteczności, aby wyeliminować błędy w komunikacji i obsłudze interfejsu. Jego praca jest kluczowa dla jakości końcowego narzędzia.

9.3.5 Główny Prawnik

Główny Prawnik analizuje zgodność systemu z przepisami (RODO, NIS2, ustawa o ochronie ludności, regulacje dot. przetwarzania danych obywateli). Opracowuje procedury zgodności i opiniuje sposób przetwarzania danych geolokalizacyjnych oraz danych wrażliwych. Monitoruje ryzyka prawne, współpracuje z cybersecurity w zakresie regulacji bezpieczeństwa. W projekcie odpowiada za minimalizowanie ryzyka prawnego na każdym etapie tworzenia systemu.

9.3.6 Specjalista szkoleń

Specjalista szkoleń przygotowuje materiały i programy szkoleniowe dla operatorów administracyjnych, służb ratunkowych oraz zespołów testowych. Prowadzi szkolenia praktyczne, testy kompetencyjne i symulacje scenariuszy kryzysowych. Opracowuje dokumentację instruktażowe (manuale, e-learning, procedury obsługi). Jego praca jest kluczowa podczas wdrożenia pilotażowego oraz późniejszych aktualizacji systemu.

9.3.7 Programista Backend

Programiści backend tworzą mikroserwisy odpowiedzialne za integrację API, logikę przetwarzania danych, system alertów i obsługę dużego obciążenia. Implementują moduły komunikacyjne, system kolejkowania zdarzeń i obsługują bazy danych. Łączą poszczególne serwisy w jedną wielką systemę - serce programu. Współpracują z DevOps oraz Technical Lead, aby utrzymać stabilność systemu. Pracują w cyklach sprintowych w pełnym wymiarze godzin.

9.3.8 Machine Learning Engineer

ML Trainer odpowiada za trenowanie modeli AI, przygotowanie zbiorów danych, tuning hiperparametrów oraz analizę jakości generowania odpowiedzi oraz wtyczek które trzeba wysłać do służb ratunkowych. Wdraża modele do infrastruktury produkcyjnej i monitoruje ich działanie pod obciążeniem. Współpracuje z data engineering oraz naukowcami od spraw kataklizmów. Rola intensywna w fazie treningów, później w trybie utrzymania.

9.3.9 Data Engineers

Inżynierowie danych projektują potoki danych, dbają o jakość, czyszczenie i normalizację informacji pobieranych z różnych API. Tworzą hurtownie danych, przygotowują strumienie near-real-time i wspierają ML przy dostarczaniu danych treningowych. Zapewniają stabilny i spójny przepływ danych między modułami. Rola kluczowa dla niezawodności systemu.

9.3.10 DevOps Engineers

DevOps inżynierowie implementują CI/CD, konfigurują chmurę, tworzą monitoring i skalowalne środowiska produkcyjne. Reagują na incydenty oraz optymalizują koszty infrastruktury. Współpracują z DevOps Lead i Technical Lead. Pracują ciągle, szczególnie intensywnie podczas wdrożeń i testów obciążeniowych.

9.3.11 Frontend Developers

Tworzą interfejs operatora, dashboardy, mapy, raporty i komponenty UI. Zapewniają responsywność, płynność działania i integrację z backendem. Współpracują z UI/UX Designerem oraz testerami, aby dopracować interfejsy.Również pomagają testerom z przetestowaniem frontu.

9.3.12 Naukowcy

Eksperci analizują poprawność logiki systemu dotyczącej konkretnych kataklizmów (pożary, powodzie, trzęsienia ziemi, burze). Weryfikują wyniki AI, pomagają ustalać progi bezpieczeństwa i interpretować dane. Biorą udział w scenariuszach testowych oraz kalibracji modeli. Są konsultantami merytorycznymi o okresowym zaangażowaniu.

9.3.13 Cybersecurity

Zespół cybersecurity odpowiada za bezpieczeństwo systemu, prowadzenie testów penetracyjnych, wdrażanie polityk IAM, szyfrowanie danych oraz audyty. Monitoruje zagrożenia i reaguje na incydenty bezpieczeństwa. Współpracuje z DevOps i prawnikiem, aby zapewnić zgodność z NIS2 i RODO. Rola kluczowa zwłaszcza po wdrożeniu systemu produkcyjnego.

9.3.14 Testerzy

Zespół testerów odpowiada za testy funkcjonalne, integracyjne, wydajnościowe oraz testy obciążeniowe przy 25 000 równoczesnych zdarzeniach. Tworzą scenariusze testowe, automatyzują testy regresyjne i raportują błędy. Pracują we wszystkich fazach projektu, od prototypów do testów końcowych TLR. Ich praca jest kluczowa dla stabilności systemu i odbioru końcowego.

9.4 Podsumowanie

W ten sposób zorganizowaliśmy naszą strukturę projektu oraz zostały wybrane poszczególne role który są niezbędnę żeby zrealizować dany projekt i z powodzeniem wdrożyć go w systemach bezpieczeństwa województw , gmin lub powiatów. Tak zrealizowany dany etap przygotowania technologicznego jest uznany za gotowy do wejścia na poziom TRL VII.

10. Prace rozwojowe – VII-IX poziom wg skali TLR.

VII poziom TLR

I. W ramach VII poziomu gotowości technologicznej zrealizowane zostaną prace badawcze w następującym zakresie:

Wprowadzenie korekt i optymalizacji wynikających z analizy odchyleń i nieścisłości wykrytych podczas testów serwerowych i użytkowych (symulacja 25 000 zdarzeń, testy z operatorami i służbami) przeprowadzonych na VI etapie gotowości technologicznej. Prace będą koncentrowały się na:

- Dalszej kalibracji modeli AI w oparciu o wyniki testów w środowisku zbliżonym do rzeczywistego, w celu podniesienia dokładności klasyfikacji zdarzeń powyżej 94%.
- Ostatecznej optymalizacji algorytmów kolejkowania i zarządzania zasobami w module Orchestratora, aby zapewnić stabilność działania przy ekstremalnym obciążeniu.
- Dopracowaniu interfejsu operatorskiego (GUI) na podstawie feedbacku od testujących operatorów centrów kryzysowych, w celu maksymalizacji intuicyjności i szybkości działania w warunkach stresu.
- Usprawnieniu mechanizmów integracji z zewnętrznymi API oraz systemami służb ratunkowych, zwiększając ich odporność na chwilowe awarie i opóźnienia.

Przeprowadzenie demonstracji systemu w rzeczywistym środowisku operacyjnym (pilotaż).

Prototyp systemu GUARDIAN zostanie wdrożony i poddany długotrwałym testom w wybranym, rzeczywistym podmiocie administracji publicznej. Test będzie obejmował:

- Rzeczywistą integrację z operacyjnymi systemami i bazami danych partnera pilotażowego.
- Monitorowanie i analizę prawdziwych, na bieżąco napływających danych ze źródeł krajowych i międzynarodowych.
- Generowanie rzeczywistych alertów testowych i treningowych dla służb ratunkowych i operatorów centrum kryzysowego.
- Weryfikację działania wszystkich modułów systemu (od integracji danych po powiadomienia) w realnych warunkach sieciowych i organizacyjnych.

II. Zakładany efekt końcowy VII poziomu gotowości technologii obejmuje następujące rezultaty:

Głównym założonym rezultatem jest pomyślne dokonanie demonstracji prototypu systemu GUARDIAN w jego docelowym, rzeczywistym środowisku operacyjnym. Osiągnięcie to stanowi bezpośredni efekt końcowy siódmego poziomu gotowości technologicznej. Oznacza to, że nastąpi praktyczna weryfikacja i prezentacja dojrzałości prototypu poprzez jego udane, długoterminowe przetestowanie w ramach pilotażu u rzeczywistego użytkownika końcowego, co ostatecznie potwierdzi gotowość technologii do pełnoskalowego wdrożenia w warunkach rzeczywistych na kolejnym, ósmym poziomie TRL.

VIII poziom TLR

I. W ramach VIII poziomu gotowości technologicznej zrealizowane zostaną prace badawcze w następującym zakresie:

- Przeprowadzenie kompleksowego pomiaru i analizy wszystkich założonych parametrów systemu (np. czas generowania alertów, dokładność AI, czas dostarczania powiadomień, stabilność) w oparciu o dane z demonstracji w środowisku operacyjnym (TRL 7).

- Bezpośrednie porównanie faktycznie uzyskanych wyników z wartościami referencyjnymi i metrykami założonymi na wcześniejszych etapach (w ujęciu do etapu VI).

- Pomiar czasu generowania alertów w realnym środowisku operacyjnym.

- Identyfikacja i analiza ewentualnych rozbieżności pomiędzy założeniami a stanem faktycznym oraz określenie ich przyczyn.

- Przygotowanie wyczerpujących i szczegółowych raportów końcowych z wszystkich przeprowadzonych pomiarów i testów walidacyjnych.

- Sformułowanie ostatecznych rekomendacji i listy niezbędnych poprawek przed pełnoskalowym wdrożeniem systemu.

Ostateczne potwierdzenie zgodności z wymaganiami prawnymi i regulacyjnymi

Zespół prawny oraz dział Cybersecurity przeprowadzą:

- końcową analizę zgodności z RODO,
- audyt wymagań dotyczących infrastruktury krytycznej,
- analizę zgodności z normami branżowymi, w tym dotyczącymi powiadamiania ludności i ochrony danych geolokalizacyjnych.

II. Zakładany efekt końcowy VIII poziomu gotowości technologii obejmuje następujące rezultaty:

- Formalne zakończenie fazy badań, rozwoju i demonstracji systemu GUARDIAN.
- Osiągnięcie ósmego poziomu gotowości technologicznej (TRL 8).
- Ostateczne potwierdzenie, że technologia systemu osiągnęła swój docelowy, gotowy do wdrożenia poziom.
- Dostarczenie kompletnej dokumentacji potwierdzającej gotowość systemu do komercjalizacji i operacyjnego użytku.

IX poziom TLR

I. W ramach IX poziomu gotowości technologicznej zrealizowane zostaną prace badawcze w następującym zakresie:

- Przygotowanie pełnej dokumentacji projektowej w ujęciu holistycznym, obejmującej specyfikacje wszystkich modułów, architekturę mikroserwisową oraz schemat komunikacji.
- Opracowanie dokumentów standardów jakościowych dla świadczonych usług, w tym metryk produktu i procedur monitoringu jakości.
- Przygotowanie kompletnej instrukcji użytkowania systemu GUARDIAN dla operatorów centrów zarządzania kryzysowego, służb ratunkowych oraz administratorów.
- Opracowanie materiałów marketingowych i biznesowych dla potencjalnych klientów z propozycją modelu sprzedażowego (umowy 5-letnie z rozliczaniem corocznym).

II. Zakładany efekt końcowy IX poziomu gotowości technologii obejmuje następujące rezultaty:

- Opracowanie kompletnej dokumentacji projektowej systemu GUARDIAN.
- Opracowanie dokumentów standardów jakościowych dla świadczonych usług.
- Opracowanie instrukcji użytkowania dla wszystkich grup użytkowników.

Efektem końcowym będzie osiągnięcie IX poziomu gotowości technologicznej. System GUARDIAN w warunkach rzeczywistych odniósł zamierzony efekt i może zostać wykorzystany komercyjnie. W związku z powyższym organizacja przejdzie do realizacji komponentu wdrożeniowego.

Zespół projektowy

Zespół projektowy odpowiedzialny za realizację systemu GUARDIAN składa się z trzech członków, z których każdy wnosi własne doświadczenie oraz kompetencje zdobyte podczas wcześniejszych projektów zespołowych, zajęć laboratoryjnych oraz samodzielnych inicjatyw technicznych. Poniżej przedstawiono doświadczenia poszczególnych członków zespołu:

Jakub Pawlak

Projekt „Wypoczynkowy”

Otrzymaliśmy wraz z drużyną projekt, który miał na celu stworzenie nowego serwisu turystycznego w oparciu o przestarzałą wersję. Wymagano od nas abyśmy zachowali stare funkcjonalności przy czym udoskonalali tam gdzie było to możliwe. Na początku jako lider porozmawiałem z każdym członkiem zespołu indywidualnie o tym jakie są ich mocne i słabe strony oraz o tym w czym czuli by się najlepiej. W ten sposób utworzyliśmy zestawienie dwóch backendowców z czego jeden był na supporcie frontenda oraz dwóch frontendowców gdzie jeden był na supporcie dla backenda. Następnie ustaliliśmy dokładny plan tego co ma być zrealizowane na kolejne tygodnie, precyzyjnie opisaliśmy a na koniec rozdzieliliśmy zadania miedzy członków drużyny. Prace przebiegały pomyślnie, co tydzień konsultowaliśmy się z klientem, który gdy coś się nie podobało informował nas na bieżąco a także zatwierdzał to co już się podobało. Przez pierwsze trzy tygodnie prace szły gładko. Niestety później zaczęła się obsówka terminowa, jeden członek zespołu nie dawał rady. Dwa dni przed prezentacją dla klienta podjęliśmy rozmowę na ten temat, gdzie kolega chodź szło mu to bardzo ciężko, twierdził, że nie ma problemu i na pewno da radę. Jak się oczywiście okazało dwa dni nie wystarczyły aby to ogarnąć, na szczęście mieliśmy dużo więcej funkcjonalności gotowych a wiec mogliśmy sobie pozwolić na lekkie opóźnienie. Członek drużyny dostał to samo zadanie na następny tydzień. W celu weryfikacji jak idą postępy, pięć dni przed terminem zapytałem się jak szły prace. Przez dwa dni cisza radiowa, nie było żadnej komunikacji. Trzy dni przed prezentacją, jak się okazuję cel został osiągnięty, a przynajmniej tak stwierdzono. Gdy przyszła próba kontrolna przed prezentacją, okazało się, że funkcjonalność nie działa i nie była dokończona. Zaczęły się nerwy, ze względu na niedomówienia. Następnego tygodnia, znowu, cisza radiowa funkcjonalność stoi w miejscu. Członek załogi wziął się za pracę dwa dni przed prezentacją. Nerwy w zespole zaczęły sięgać apogeum gdy nawet ja jako lider straciłem zimną krew, zaczęły się konflikty. Przy prezentacji nie wyglądało to najlepiej ale na szczęście reszta funkcjonalności była wystarczająca aby osiągnąć zadowalający poziom. Ostatni tydzień tego zadania mimo protestów spóźnialskiego zdecydowaliśmy, że kilka osób podejmie się pomocy przy realizacji tego zadania. Na ten tydzień już mieliśmy tą funkcjonalność, jednak konflikty powstałe w zespole przez tą sytuacje zrodziły ciemne chmury wiszące nad zespołem. Pozostał lekki niesmak który towarzyszył nam aż do końca projektu. Finalnie projekt zakończył się powodzeniem, mimo czterotygodniowego opóźnienia z zadaniem.

Wnioski: W sytuacji w której w projekcie rodzi się zastój, należy głębiej się przyjrzeć problemowi i lepiej porozumieć się z osobą odpowiedzialną za zadanie. Niedomówienia, duma, czy jakakolwiek inna bariera nie powinna stać na przeszkodzie realizacji projektu. Lepiej jest poświęcić trochę więcej czasu na rozmowę oraz zadbać o poprawną komunikację niż pozwolić na szerzenie się negatywnych emocji w zespole. To właśnie lider powinien sprawować pieczę nad tym zadaniem a także zawsze mieć zachowaną zimną krew. Należy pamiętać też, że do komunikacji potrzeba dwóch osób.

Ruslan Zhukotynskyi

Projekt z rozpoznawania znaków drogowych
Podczas zajęć na studiach inżynierskich naszym zadaniem było zrealizowanie projektu dla firmy Visimind. Celem było stworzenie aplikacji mobilnej umożliwiającej rozpoznawanie znaków drogowych zarówno na zdjęciach, jak i w czasie rzeczywistym. Na wykonanie projektu przeznaczono 13 tygodni (160 godzin pracy zespołowej).

W skład zespołu wchodziło 5 osób, które podzieliły się rolami:
– 2 frontend developerów,
– 2 backend developerów,
– 1 osoba odpowiedzialna za Machine Learning.

Prace rozpoczęliśmy od zapoznania się z technologiami, których wcześniej nie używaliśmy. Był to etap wymagający, gdyż nauka nowych narzędzi pochłonęła dużo czasu. Następnie otrzymaliśmy od firmy treningowy zbiór danych, który został podzielony pomiędzy grupami w celu szybszego i efektywniejszego labelowania. Każdy z członków zespołu miał przydzielone zadania wraz z harmonogramem realizacji. Pomimo przygotowanego planu, pojawiły się trudności w dotrzymywaniu terminów, głównie z powodu ograniczonego czasu (inne zajęcia na uczelni i dodatkowe projekty). Dodatkowym problemem był fakt, że lider zespołu nie egzekwował systematycznej kontroli postępów, co negatywnie wpłynęło na tempo pracy. Gdy frontend i backend osiągnęły już podstawową funkcjonalność, moim zadaniem było ich integracja. Po pierwszym udanym połączeniu zaprezentowaliśmy wersję demo firmie, która wskazała błędy oraz możliwe ulepszenia. W szczególności zwrócono uwagę na konieczność wdrożenia modelu ML bezpośrednio w aplikacji (w formacie .tflite), zamiast przesyłania zapytań do API co sekundę – rozwiązanie to było nieefektywne i generowało opóźnienia.W końcowej fazie projektu, po dopracowaniu frontendu i backendu, zająłem się powiększeniem zbioru danych w celu poprawy dokładności modelu. Współpracowałem również z członkiem innej grupy przy tworzeniu programu do automatycznego labelowania. Dzięki temu udało się znacząco usprawnić proces przygotowania danych. Finalnie backendowcy wyeksportowali wytrenowany model i wdrożyli go w aplikacji mobilnej. Na zakończenie wspólnie opracowaliśmy dokumentację. W dniu oddania projektu odbyła się prezentacja naszej aplikacji – przedstawiliśmy proces tworzenia oraz zaprezentowaliśmy działanie systemu na żywo. Firma była zadowolona z rezultatów, choć nie udało się wdrożyć funkcji wykrywania znaków na nagraniach wideo, a cały projekt ukończyliśmy w ostatnim możliwym terminie.

Wnioski: W procesie planowania projektu nie zostały uwzględnione czynniki ludzkie ani ryzyka związane z możliwością niedotrzymania terminów, dlatego nie zaplanowaliśmy wersji „lite" aplikacji, która spełniałaby minimalne wymagania projektowe. Zamiast tego od razu podjęliśmy się realizacji dużych zadań, z których część ostatecznie musieliśmy porzucić. Dodatkowym problemem było to, że team leader nie kontrolował regularnie postępów – nie sprawdzał cotygodniowo efektów pracy poszczególnych członków zespołu, a czasem całkowicie to odpuszczał. W końcowych etapach projektu konieczne były drobne konflikty i spory, aby zmobilizować wszystkich do intensywniejszej pracy i uzyskać satysfakcjonujący rezultat. Choć każdy miał wyznaczoną swoją część zadań, w praktyce okazało się, że niektórzy musieli poświęcać więcej czasu i przejmować obowiązki za innych, którzy nie zrealizowali swoich komponentów. W rezultacie można stwierdzić, że w przyszłości konieczne jest lepsze planowanie zadań i harmonogramu, a także uwzględnianie możliwych problemów oraz przygotowanie alternatywnych scenariuszy. Tylko w ten sposób można uniknąć sytuacji, w której projekt kończony jest w pośpiechu i wymaga improwizowanych rozwiązań.

Remigiusz Sęk

System służący do automatycznej klasyfikacji i mapowania upraw
Moje doświadczenie dotyczy realizacji innowacyjnego projektu stażowego w jednej z wiodących firm sektora kosmicznego. Zadaniem było stworzenie systemu służącego do automatycznej klasyfikacji i mapowania upraw na podstawie danych satelitarnych Sentinel-1 i Sentinel-2, z wykorzystaniem nowoczesnego modelu typu Foundation Model (opracowanego przez NASA Harvest). Było to moje pierwsze zetknięcie z tą specyficzną i zaawansowaną technologią

Projekt rozpocząłem od solidnego przygotowania merytorycznego. Przeprowadziłem research dostępnych rozwiązań, zapoznałem się z dokumentacją i przygotowałem środowisko pracy. Jednakże, ze względu na nowatorski charakter technologii, początkowo przyjąłem standardowe podejście do implementacji, które sprawdzało się w klasycznych modelach uczenia maszynowego. Skupiłem się na szybkim uruchomieniu prototypu, aby zweryfikować działanie systemu w praktyce ("Proof of Concept")

W trakcie prac okazało się, że specyfika Foundation Modelu wymaga znacznie głębszego zejścia w techniczne detale architektury niż zakładałem. Mimo poprawnego przygotowania ogólnego, moje założenia dotyczące formatu danych wejściowych (embeddingów) wymagały rewizji. Model, oparty na zaawansowanym mechanizmie uwagi (attention), przetwarzał dane w sposób kontekstowy (całe wycinki obrazu), a nie punktowy, co odkryłem dzięki wnikliwej analizie zachowania systemu.

To doświadczenie było kluczową lekcją, która pozwoliła mi zrozumieć różnicę między badaniami ogólnymi a deep-tech wymaganymi przy pracy z technologiami klasy "cutting-edge". Czas poświęcony na refaktoryzację kodu nie był stracony – pozwolił mi na dogłębne zrozumienie architektury Transformerów w danych geoprzestrzennych, co jest unikalną kompetencją na rynku. Wyciągnięte wnioski natychmiast przekułem w sukces w kolejnym projekcie konkursowym (realizowanym w ramach programu dużej firmy technologicznej), gdzie jako zespół z koła naukowego zajęliśmy miejsce na podium. Tam, bogatszy o doświadczenie, od razu przygotowałem precyzyjny Low-Level Design, co pozwoliło na bezbłędną i efektywną implementację.

Wnioski:

- **Specyfika nowych technologii**: Przy wdrażaniu rozwiązań, z którymi stykamy się po raz pierwszy (jak Foundation Models), standardowy research może być niewystarczający. Należy uwzględnić dodatkowy czas na tzw. "deep dive" techniczny, czyli analizę architektury rozwiązania na najniższym poziomie (Low-Level Design)
- **Jakość vs. Ilość informacji**: Solidny research to nie tylko zgromadzenie dużej ilości materiałów, ale przede wszystkim ich techniczna weryfikacja pod kątem konkretnego zastosowania (Use Case). Tworzenie tabel porównawczych z parametrami technicznymi (np. format tensorów wejściowych, wymagania pamięciowe) pozwala uniknąć pułapek implementacyjnych.
- **Ewolucyjne podejście do projektu**: Konieczność zmiany podejścia w trakcie projektu nie jest porażką, lecz naturalnym elementem pracy badawczo-rozwojowej (R&D). Kluczem do sukcesu jest szybka identyfikacja rozbieżności i adaptacja planu, co w moim przypadku doprowadziło do głębszego zrozumienia technologii.
- **Dokumentacja jako narzędzie analityczne**: Tworzenie dokumentacji technicznej i schematów przepływu danych (Data Flow Diagrams) przed rozpoczęciem kodowania pozwala zweryfikować poprawność założeń i jest kluczowe w projektach o wysokim stopniu skomplikowania.

- **Weryfikacja poprzez eksperyment**: Najlepszym uzupełnieniem teoretycznego researchu są szybkie eksperymenty na małej skali. Pozwalają one potwierdzić, czy nasze rozumienie dokumentacji pokrywa się z rzeczywistym działaniem bibliotek i modeli.

Symulacja projektu informatycznego Global Unified Automated Response and Disaster Intelligence Alert Network (GUARDIAN)

W ramach realizacji projektu opracowano pełny model finansowy obejmujący koszty jednorazowe, koszty stałe oraz prognozowane przychody, zgodnie z wymaganiami symulacji wdrożenia systemu GUARDIAN. Na podstawie wzorca budżetu dokonano jego modyfikacji, dostosowując strukturę i obliczenia do specyfiki naszego projektu oraz jego rzeczywistych potrzeb technologicznych i organizacyjnych.

Wszystkie wartości finansowe zostały przedstawione zarówno w złotówkach (PLN), jak i w dolarach (USD), aby umożliwić porównywalność kosztów oraz uwzględnić potencjalne rozliczenia z partnerami zagranicznymi. Na potrzeby kalkulacji przyjęto aktualny kurs walutowy:

1 USD = 3,65 PLN

Przyjęty kurs został zastosowany konsekwentnie we wszystkich pozycjach kosztowych oraz przychodowych, co zapewnia spójność finansową całego budżetu. Opracowany model finansowy umożliwia analizę Cash Flow dla okresu 24 i 36 miesięcy, wraz z wyznaczeniem punktu rentowności oraz zwrotu inwestycji.

1. Średnia cena za produkt

Średnia cena za produkt		
średni zysk z użytkownika za wdrożenie systemu	$90 410,96	330 000,00zł
średni zysk z użytkownika za obsługę techniczną na miesiąc	$2 191,78	8 000,00 zł

2. Ilość sprzedanych aplikacji w sprzedaży bezpośredniej

Ilość sprzedanych aplikacji w sprzedaży bezpośredniej							
Miesiąc	**Ilość zakupów**	**Wdrożenie w ZŁ**	**Wdrożenie w USD**	**Maintenance w ZŁ**	**Maintenance w USD**	**Przychód na miesiąc w ZŁ**	**Przychód na miesiąc w USD**
1	1	330 000,00zł	$90 410,96			330 000,00zł	$90 410,96
2	0	0,00zł	$0,00	8 000,00 zł	$2 191,78	8 000,00zł	$2 191,78
3	2	660 000,00zł	$180 821,92	8 000,00 zł	$2 191,78	668 000,00zł	$183 013,70

4	0	0,00zł	$0,00	24 000,00 zł	$6 575,34	24 000,00zł	$6 575,34
5	0	0,00zł	$0,00	24 000,00 zł	$6 575,34	24 000,00zł	$6 575,34
6	3	990 000,00zł	$271 232,88	24 000,00 zł	$6 575,34	1 014 000,00zł	$277 808,22
7	0	0,00zł	$0,00	48 000,00 zł	$13 150,68	48 000,00zł	$13 150,68
8	0	0,00zł	$0,00	48 000,00 zł	$13 150,68	48 000,00zł	$13 150,68
9	2	660 000,00zł	$180 821,92	48 000,00 zł	$13 150,68	708 000,00zł	$193 972,60
10	0	0,00zł	$0,00	64 000,00 zł	$17 534,25	64 000,00zł	$17 534,25
11	0	0,00zł	$0,00	64 000,00 zł	$17 534,25	64 000,00zł	$17 534,25
12	5	1 650 000,00zł	$452 054,79	64 000,00 zł	$17 534,25	1 714 000,00zł	$469 589,04
13	1	330 000,00zł	$90 410,96	104 000,00 zł	$28 493,15	434 000,00zł	$118 904,11
14	2	660 000,00zł	$180 821,92	112 000,00 zł	$30 684,93	772 000,00zł	$211 506,85
15	0	0,00zł	$0,00	128 000,00 zł	$35 068,49	128 000,00zł	$35 068,49
16	0	0,00zł	$0,00	128 000,00 zł	$35 068,49	128 000,00zł	$35 068,49
17	3	990 000,00zł	$271 232,88	128 000,00 zł	$35 068,49	1 118 000,00zł	$306 301,37
18	2	660 000,00zł	$180 821,92	152 000,00 zł	$41 643,84	812 000,00zł	$222 465,75
19	5	1 650 000,00zł	$452 054,79	168 000,00 zł	$46 027,40	1 818 000,00zł	$498 082,19
20	0	0,00zł	$0,00	208 000,00 zł	$56 986,30	208 000,00zł	$56 986,30
21	0	0,00zł	$0,00	208 000,00 zł	$56 986,30	208 000,00zł	$56 986,30
22	1	330 000,00zł	$90 410,96	208 000,00 zł	$56 986,30	538 000,00zł	$147 397,26
23	1	330 000,00zł	$90 410,96	216 000,00 zł	$59 178,08	546 000,00zł	$149 589,04
24	6	1 980 000,00zł	$542 465,75	224 000,00 zł	$61 369,86	2 204 000,00zł	$603 835,62
25	5	1 650 000,00zł	$452 054,79	272 000,00 zł	$74 520,55	1 922 000,00zł	$526 575,34
26	4	1 320 000,00zł	$361 643,84	312 000,00 zł	$85 479,45	1 632 000,00zł	$447 123,29
27	2	660 000,00zł	$180 821,92	344 000,00 zł	$94 246,58	1 004 000,00zł	$275 068,49
28	1	330 000,00zł	$90 410,96	360 000,00 zł	$98 630,14	690 000,00zł	$189 041,10
29	1	330 000,00zł	$90 410,96	368 000,00 zł	$100 821,92	698 000,00zł	$191 232,88
30	6	1 980 000,00zł	$542 465,75	376 000,00 zł	$103 013,70	2 356 000,00zł	$645 479,45
31	3	990 000,00zł	$271 232,88	424 000,00 zł	$116 164,38	1 414 000,00zł	$387 397,26
32	2	660 000,00zł	$180 821,92	448 000,00 zł	$122 739,73	1 108 000,00zł	$303 561,64
33	1	330 000,00zł	$90 410,96	464 000,00 zł	$127 123,29	794 000,00zł	$217 534,25
34	3	990 000,00zł	$271 232,88	472 000,00 zł	$129 315,07	1 462 000,00zł	$400 547,95
35	2	660 000,00zł	$180 821,92	496 000,00 zł	$135 890,41	1 156 000,00zł	$316 712,33
36	3	990 000,00zł	$271 232,88	512 000,00 zł	$140 273,97	1 502 000,00zł	$411 506,85
Razem	**67**	**22 110 000,00 zł**	**6 057 534,25 zł**	**7 256 000,00 zł**	**$1 987 945,21**	**29 366 000,00zł**	**$8 045 479,45**

3. Koszty miesięczne I rok projektu

Koszty miesięczne I rok projektu					
Lp.	**nazwa**	**Ilość**	**kwota brutto za 1 szt**	**Kwota brutto razem**	**Uwagi**
1	API	6	0,00 zł	0,00 zł	To są otwarte dane
2	Wynagrodzenie programista backend	3	12 500,00 zł	37 500,00 zł	Rozkładamy na comiesięczne rozliczanie z programistami
3	Wynagrodzenie programista frontend	2	8 000,00 zł	16 000,00 zł	Płatność junioram
4	Wynagrodzenie programista ML	2	17 000,00 zł	34 000,00 zł	Płatność doświadczonym ML programistam.
5	Wynagrodzenie tester	3	9 000,00 zł	27 000,00 zł	Płatność na zlecenie
6	Wynagrodzenie cybersecurity	2	13 000,00 zł	26 000,00 zł	Koszt z ZUS
7	Wynagrodzenie Data Engineering	2	8 500,00 zł	17 000,00 zł	Koszt z ZUS
8	Wynagrodzenie DevOps	2	10 000,00 zł	20 000,00 zł	Koszt z ZUS
9	Wynagrodzenie Naukowca	3	6 000,00 zł	18 000,00 zł	Koszt z ZUS
10	Wynagrodzenie Prawnik	1	14 500,00 zł	14 500,00 zł	Koszt z ZUS
11	Wynagrodzenie kierowników grup	4	16 000,00 zł	64 000,00 zł	Koszt z ZUS
12	Abonament światłowodowy	1	200,00 zł	200,00 zł	Dobry abonament dla dobrego zasięgu
13	Licencja na zarządzanie bazą danych	1	2 000,00 zł	2 000,00 zł	Współpracujemy z systemem zarządzania bazą danych
14	Licencja na środowisko chmurowe	1	2 000,00 zł	2 000,00 zł	Backups
15	Wynagrodzenie Marketingowiec i PR	1	12 500,00 zł	12 500,00 zł	koszt z ZUS
16	Księgowość	1	3 000,00 zł	3 000,00 zł	
17	Serwery	14	1 100,00 zł	15 400,00 zł	3 na dane, 3 na kolejkę zdarzeń, 4 na AI, 2 na monitoring, 1 na środowisko testowe, serwer kopii 1
18	Marketing i reklama	1	36 000,00 zł	36 000,00 zł	
19	Wynajem biura	2	6 000,00 zł	12 000,00 zł	Biuro w Olsztynie oraz Warszawie

20	Inne	1	8 000,00 zł	8 000,00 zł	Kawa, herbata, prąd, materiały biurowe, tonnery do drukarek, papier, znaczki, paczki itp.
		Razem	**185 300,00 zł**	**365 100,00 zł**	

4. Koszty miesięczne II rok projektu

Koszty miesięczne II rok projektu					
Lp.	**nazwa**	**Ilość**	**kwota brutto za 1 szt**	**Kwota brutto razem**	**Uwagi**
1	API	6	0,00 zł	0,00 zł	To są otwarte dane
2	Wynagrodzenie programista backend	3	12 500,00 zł	37 500,00 zł	Rozkładamy na comiesięczne rozliczanie z programistami
3	Wynagrodzenie programista frontend	2	8 000,00 zł	16 000,00 zł	Płatność junioram
4	Wynagrodzenie programista ML	2	17 000,00 zł	34 000,00 zł	Płatność doświadczonym ML programistam.
5	Wynagrodzenie tester	2	11 500,00 zł	23 000,00 zł	Płatność na zlecenie
6	Wynagrodzenie cybersecurity	2	13 000,00 zł	26 000,00 zł	Koszt z ZUS
7	Wynagrodzenie Data Engineering	2	8 500,00 zł	17 000,00 zł	Koszt z ZUS
8	Wynagrodzenie DevOps	1	14 000,00 zł	14 000,00 zł	Koszt z ZUS
9	Wynagrodzenie Naukowca	3	6 000,00 zł	18 000,00 zł	Koszt z ZUS
10	Wynagrodzenie Prawnik	1	14 500,00 zł	14 500,00 zł	Koszt z ZUS
11	Wynagrodzenie kierowników grup	4	16 000,00 zł	64 000,00 zł	Koszt z ZUS
12	Abonament światłowodowy	1	220,00 zł	220,00 zł	Dobry abonament dla dobrego zasięgu
13	Licencja na zarządzanie bazą danych	1	2 000,00 zł	2 000,00 zł	Współpracujemy z systemem zarządzania bazą danych
14	Licencja na środowisko chmurowe	1	2 000,00 zł	2 000,00 zł	Backups
15	Wynagrodzenie Marketingowiec i PR	1	12 500,00 zł	12 500,00 zł	koszt z ZUS
16	Księgowość	1	3 000,00 zł	3 000,00 zł	

17	Serwery	19	1 200,00 zł	22 800,00 zł	5 na dane, 4 na kolejkę zdarzeń, 4 na AI, 3 na monitoring, 2 na środowisko testowe, serwer kopii 1
18	Marketing i reklama	1	46 000,00 zł	46 000,00 zł	
19	Wynajem biura	2	6 000,00 zł	12 000,00 zł	Biuro w Olsztynie oraz Warszawie
20	Inne	1	6 000,00 zł	6 000,00 zł	Kawa, herbata, prąd, materiały biurowe, tonnery do drukarek, papier, znaczki, paczki itp.
		Razem	**199 920,00 zł**	**370 520,00 zł**	

5. Koszty miesięczne III rok projektu

Koszty miesięczne III rok projektu					
Lp.	**nazwa**	**Ilość**	**kwota brutto za 1 szt**	**Kwota brutto razem**	**Uwagi**
1	API	6	0,00 zł	0,00 zł	To są otwarte dane
2	Wynagrodzenie programista backend	4	16 500,00 zł	66 000,00 zł	Rozkładamy na comiesięczne rozliczanie z programistami
3	Wynagrodzenie programista frontend	2	8 000,00 zł	16 000,00 zł	Płatność junioram
4	Wynagrodzenie programista ML	3	17 000,00 zł	51 000,00 zł	Płatność doświadczonym ML programistam.
5	Wynagrodzenie tester	2	11 500,00 zł	23 000,00 zł	Płatność na zlecenie
6	Wynagrodzenie cybersecurity	2	13 000,00 zł	26 000,00 zł	Koszt z ZUS
7	Wynagrodzenie Data Engineering	2	8 500,00 zł	17 000,00 zł	Koszt z ZUS
8	Wynagrodzenie DevOps	1	14 000,00 zł	14 000,00 zł	Koszt z ZUS
9	Wynagrodzenie Naukowca	3	7 000,00 zł	21 000,00 zł	Koszt z ZUS
10	Wynagrodzenie Prawnik	2	15 500,00 zł	31 000,00 zł	Koszt z ZUS
11	Wynagrodzenie kierowników grup	4	19 000,00 zł	76 000,00 zł	Koszt z ZUS
12	Abonament światłowodowy	1	300,00 zł	300,00 zł	Dobry abonament dla dobrego zasięgu
13	Licencja na zarządzanie bazą danych	1	2 000,00 zł	2 000,00 zł	Współpracujemy z systemem zarządzania bazą danych
14	Licencja na środowisko chmurowe	1	2 000,00 zł	2 000,00 zł	Backups

15	Wynagrodzenie Marketingowiec i PR	1	13 500,00 zł	13 500,00 zł	koszt z ZUS
16	Księgowość	1	3 000,00 zł	3 000,00 zł	
17	Serwery	30	1 200,00 zł	36 000,00 zł	11 na dane, 7 na kolejkę zdarzeń, 5 na AI, 3 na monitoring, 2 na środowisko testowe, serwer kopii 2
18	Marketing i reklama	1	70 000,00 zł	70 000,00 zł	
19	Wynajem biura	3	6 000,00 zł	18 000,00 zł	Biuro w Olsztynie oraz Warszawie i Gdańsku
20	Inne	1	6 000,00 zł	6 000,00 zł	Kawa, herbata, prąd, materiały biurowe, tonnery do drukarek, papier, znaczki, paczki itp.
		Razem	**234 000,00 zł**	**491 800,00 zł**	

6. Koszty jednorazowe I rok projektu

Koszty jednorazowe I rok projektu					
Lp.	**nazwa**	**Ilość**	**kwota brutto za 1 szt**	**Kwota brutto razem**	**Uwagi**
1	Komputery z silnym GPU	3	25 000,00 zł	75 000,00 zł	Mocne komputery obliczeniowe
2	Dostęp światłowodowy	1	1 400,00 zł	1 400,00 zł	Internet
3	Stanowiska komputerowe dla programowania	16	12 000,00 zł	192 000,00 zł	Komputery dla pozostałych pracowników
3	Pozostałe rzeczy wyposażenia biura	1	5 000,00 zł	5 000,00 zł	Fotel, Ekrany, Table Tennis
			Razem	**268 400,00 zł**	

7. Koszty jednorazowe II rok projektu

Koszty jednorazowe II rok projektu					
Lp.	**nazwa**	**Ilość**	**kwota brutto za 1 szt**	**Kwota brutto razem**	**Uwagi**
1	Dostęp światłowodowy	1	2 000,00 zł	2 000,00 zł	Lepszy internet
2	Stanowiska komputerowe dla programowania	4	12 000,00 zł	48 000,00 zł	Dodatkowe

3	Gry	1	3 000,00 zł	3 000,00 zł	Żeby można było zrobić rozrywkę
4	Pozostałe rzeczy wyposażenia biura	1	5 000,00 zł	5 000,00 zł	
			Razem	**58 000,00 zł**	

8. Koszty jednorazowe III rok projektu

Koszty jednorazowe III rok projektu					
Lp.	**nazwa**	**Ilość**	**kwota brutto za 1 szt**	**Kwota brutto razem**	**Uwagi**
1	Komputery z silnym GPU	1	25 000,00 zł	25 000,00 zł	Jeszcze jeden ML
2	Stanowiska komputerowe dla programowania	1	12 000,00 zł	12 000,00 zł	Zapas
3	Aktualizacja lub wymiana sprzętu komputerowego	1	200 000,00 zł	200 000,00 zł	W razie potrzeby naprawy
4	Pozostałe rzeczy wyposażenia biura	1	7 000,00 zł	7 000,00 zł	
			Razem	**244 000,00 zł**	

9. Cashflow

Cashflow						
Miesiąc	**Łączna ilość sprzedanych aplikacji**	**Przychód brutto**	**Koszt miesięczny**	**Koszt jednorazowy**	**Bilans zysku w miesiącu**	**Bilans razem (zysk łączny)**
1	1	330 000,00 zł	365 100,00 zł	268 400,00 zł	**-303 500,00 zł**	**-303 500,00 zł**
2	0	8 000,00 zł	365 100,00 zł	0,00 zł	**-357 100,00 zł**	**-660 600,00 zł**
3	2	668 000,00 zł	365 100,00 zł	0,00 zł	302 900,00 zł	**-357 700,00 zł**

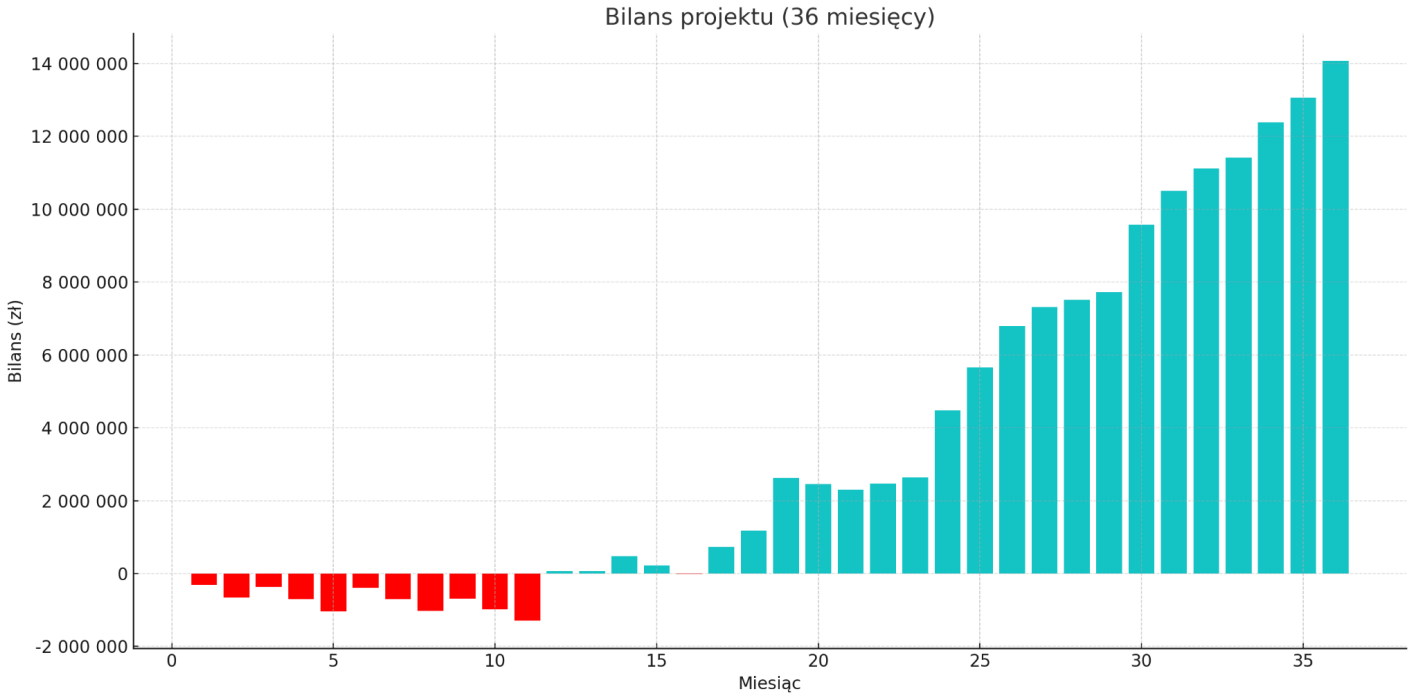
4	0	24 000,00 zł	365 100,00 zł	0,00 zł	**-341 100,00 zł**	**-698 800,00 zł**
5	0	24 000,00 zł	365 100,00 zł	0,00 zł	**-341 100,00 zł**	**-1 039 900,00 zł**
6	3	1 014 000,00 zł	365 100,00 zł	0,00 zł	648 900,00 zł	**-391 000,00 zł**
7	0	48 000,00 zł	365 100,00 zł	0,00 zł	**-317 100,00 zł**	**-708 100,00 zł**
8	0	48 000,00 zł	365 100,00 zł	0,00 zł	**-317 100,00 zł**	**-1 025 200,00 zł**
9	2	708 000,00 zł	365 100,00 zł	0,00 zł	342 900,00 zł	**-682 300,00 zł**
10	0	64 000,00 zł	365 100,00 zł	0,00 zł	**-301 100,00 zł**	**-983 400,00 zł**
11	0	64 000,00 zł	365 100,00 zł	0,00 zł	**-301 100,00 zł**	**-1 284 500,00 zł**
12	5	1 714 000,00 zł	365 100,00 zł	0,00 zł	1 348 900,00 zł	64 400,00 zł
13	1	434 000,00zł	370 520,00 zł	58 000,00 zł	5 480,00 zł	69 880,00 zł
14	2	772 000,00zł	370 520,00 zł	0,00 zł	401 480,00 zł	471 360,00 zł
15	0	128 000,00zł	370 520,00 zł	0,00 zł	**-242 520,00 zł**	228 840,00 zł
16	0	128 000,00zł	370 520,00 zł	0,00 zł	**-242 520,00 zł**	**-13 680,00 zł**
17	3	1 118 000,00zł	370 520,00 zł	0,00 zł	747 480,00 zł	733 800,00 zł

18	2	812 000,00zł	370 520,00 zł	0,00 zł	441 480,00 zł	1 175 280,00 zł
19	5	1 818 000,00zł	370 520,00 zł	0,00 zł	1 447 480,00 zł	2 622 760,00 zł
20	0	208 000,00zł	370 520,00 zł	0,00 zł	**-162 520,00 zł**	2 460 240,00 zł
21	0	208 000,00zł	370 520,00 zł	0,00 zł	**-162 520,00 zł**	2 297 720,00 zł
22	1	538 000,00zł	370 520,00 zł	0,00 zł	167 480,00 zł	2 465 200,00 zł
23	1	546 000,00zł	370 520,00 zł	0,00 zł	175 480,00 zł	2 640 680,00 zł
24	6	2 204 000,00zł	370 520,00 zł	0,00 zł	1 833 480,00 zł	4 474 160,00 zł
25	5	1 922 000,00zł	491 800,00 zł	244 000,00 zł	1 186 200,00 zł	5 660 360,00 zł
26	4	1 632 000,00zł	491 800,00 zł	0,00 zł	1 140 200,00 zł	6 800 560,00 zł
27	2	1 004 000,00zł	491 800,00 zł	0,00 zł	512 200,00 zł	7 312 760,00 zł
28	1	690 000,00zł	491 800,00 zł	0,00 zł	198 200,00 zł	7 510 960,00 zł
29	1	698 000,00zł	491 800,00 zł	0,00 zł	206 200,00 zł	7 717 160,00 zł
30	6	2 356 000,00zł	491 800,00 zł	0,00 zł	1 864 200,00 zł	9 581 360,00 zł
31	3	1 414 000,00zł	491 800,00 zł	0,00 zł	922 200,00 zł	10 503 560,00 zł

32	2	1 108 000,00zł	491 800,00 zł	0,00 zł	616 200,00 zł	11 119 760,00 zł
33	1	794 000,00zł	491 800,00 zł	0,00 zł	302 200,00 zł	11 421 960,00 zł
34	3	1 462 000,00zł	491 800,00 zł	0,00 zł	970 200,00 zł	12 392 160,00 zł
35	2	1 156 000,00zł	491 800,00 zł	0,00 zł	664 200,00 zł	13 056 360,00 zł
36	3	1 502 000,00zł	491 800,00 zł	0,00 zł	1 010 200,00 zł	14 066 560,00 zł
Razem	**67**	**29 366 000,00 zł**	**14 729 040,00 zł**	**570 400,00 zł**		

Na podstawie przeprowadzonych obliczeń finansowych dla okresu 36 miesięcy można zauważyć, że projekt osiąga **punkt rentowności po około 12 miesiącach**, natomiast faktyczny **zwrot z inwestycji** zaczyna się materializować dopiero w kolejnych miesiącach, gdy przychody rosną szybciej niż koszty operacyjne. Analiza przepływów pieniężnych wskazuje, że w pierwszym roku projekt generuje znaczące obciążenie finansowe, które stopniowo maleje wraz z wejściem systemu na rynek i pozyskiwaniem klientów.

W oparciu o zsumowane wartości ujemnych przepływów pieniężnych w pierwszych miesiącach można określić, że **minimalny wymagany kapitał początkowy**, pozwalający bezpiecznie przeprowadzić projekt przez najbardziej kosztowne etapy budowy i wdrażania systemu, wynosi **około 1 300 000 zł**. Taka kwota gwarantuje utrzymanie płynności finansowej w okresie przed komercyjnym oraz umożliwia prowadzenie aktywnych działań sprzedażowych i marketingowych w celu pozyskania pierwszych klientów.



W dalszych etapach można rozszerzyć nasz system na inne kraje i w końcu osiągnąć poziom Światowego GUARDIAN! Możliwe że to się uda!