Project Design Document

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

Przedmiot: Zarządzanie projektem informatycznym

Grupa nr: 2

Zespół:

- Ruslan Zhukotynskyi - kierownik
- Remigiusz Sęk
- Jakub Pawlak

Spis treści:

1. Lab 2

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. Lab 3

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 (fusion API), 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. Lab 4

W ramach III poziomu gotowości technologicznej systemu GUARDIAN-AI 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. Lab 5

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-AI 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 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. Lab 6

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 i gminy.

Model biznesowy (sprzedażowy) - System będzie sprzedawany dla podmiotów z umową na 5 lat użytkowania z rozliczaniem corocznym. 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. Lab 7 - 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 nieoptymalnymi 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 poprawnosci przesylania komunikatow 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 kompletnosc przekazywanych danych (lokalizacja, intensywnosc zjawiska, rekomendowane działania i wyposażenie), czas dostarczenia komunikatu oraz poprawnosc potwierdzeń odbioru. Zidentyfikowano pojedyncze przypadki błędnych certyfikatów uwierzytelniających, które powodowały odrzucenie żądania przez serwer odbiorcy. Po ponownej konfiguracji certyfikatów i aktualizacji schematu integracji komunikaty były poprawnie przekazywane do wszystkich odbiorców a sredni czas dostarczenia wynósł poniżej 5 sekund.

6.6 Moduł informowania obywateli

Dokonano integracji modułu informowania obywateli z centralnym orchestratorem systemu. Przeprowadzono testy poprawnosci wysylki komunikatow ostrzegawczych do obywateli na podstawie danych geolokalizacyjnych w srodowisku testowym obejmujacym 10 stref geograficznych. Test wykonano z wykorzystaniem symulowanego dostawcy usług SMS i e-mail dla 5000 numerów testowych. Weryfikowano poprawnosc selekcji odbiorcow, kompletnosc i czytelnosc tresci komunikatow 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 tescie wszystkie komunikaty zostaly poprawnie dostarzcone do wlasciwych adresatow w czasie ponizej 30 sekund.

7. Lab 8 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 katalkizmów (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 spóźnione 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 poprawi 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. Lab 9. Badania przemysłowe

8.1 Model prototypu w warunkach zbliżonych do rzeczywistych

Przeprowadzono pełną integrację wszystkich sześciu modułów systemu GUARDIAN-AI 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. gmin, 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-AI**, 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 co 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

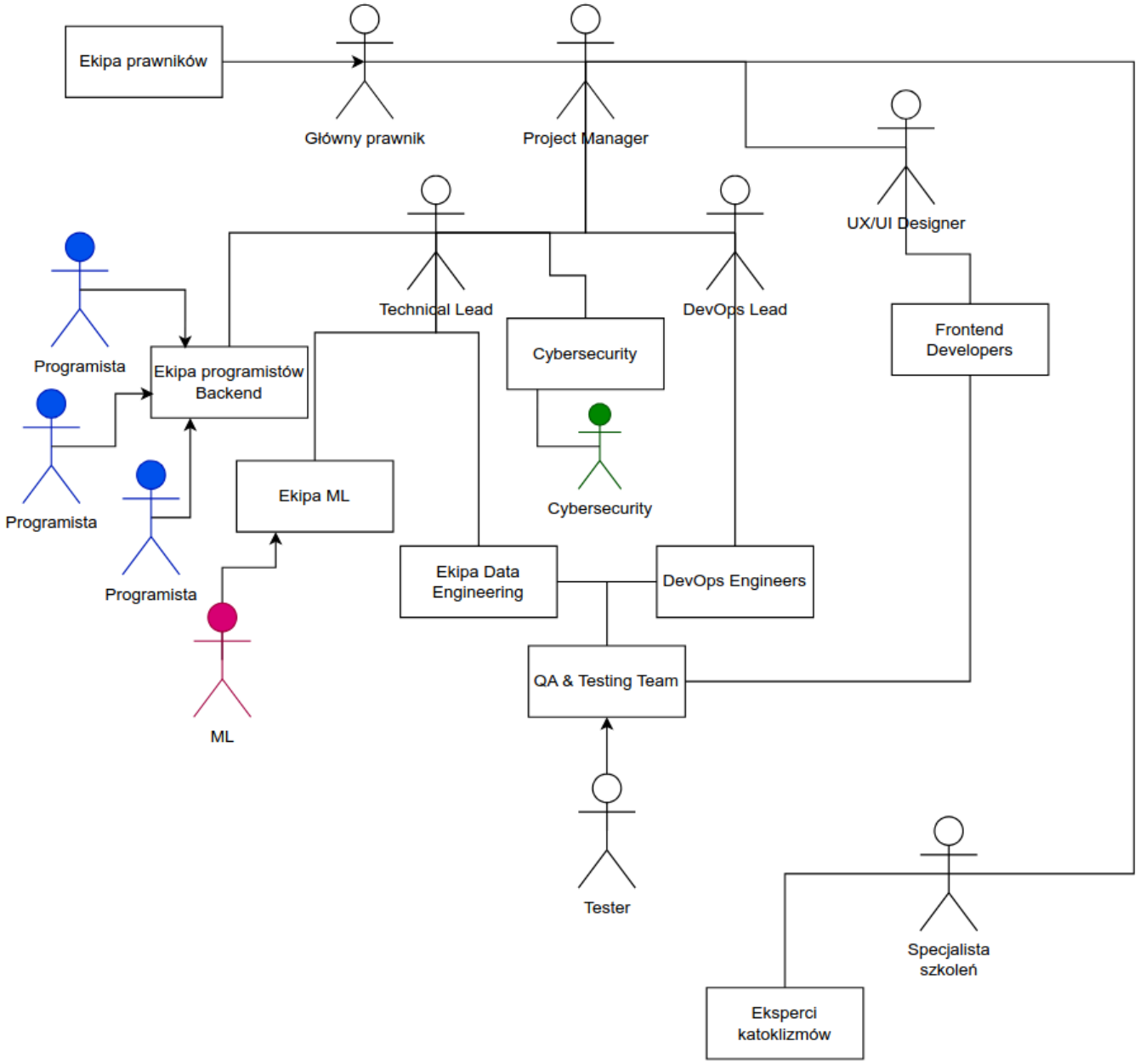
czasu dotarcia oraz intensywności zdarzeń, tak aby jedna jednostka mogła obsłużyć kilka punktów, jeśli jest to możliwe, a nadmiarowe jednostki nie były wysyłane tam, gdzie nie są potrzebne.

9. Lab 10. Zarządzanie jakością i struktura organizacyjna projektu

9.1 Metryka produktu

Metryka produktu: System wczesnego ostrzegania GUARDIAN-AI		
Czas generowania alertu od wykrycia zdarzenia	7 sekund	Sredni czas od detekcji kataklizmu do wyslania alertu
Czas dostarczenia SMS do obywatela	30 sekund	Pomiar z systemu SMS gateway
Skutecznosc dostarczenia alertow	99%	Procent skutecznie dostarczonych wiadomosci
Czas reakcji interfejsu operatorskiego	5 sekund	Sredni czas ladowania i reakcji GUI dla operatora
Dokładnosc klasyfikacji zdarzen AI	94%	Test na zbiorze kontrolnym zdarzeń
Stabilnosc systemu pod obciazeniem (25 000)	Bez bledow krytycznych	Test obciazenia 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, orkiestrator, 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 gmin, powiatów, służb ratunkowych oraz panel analiz AI. 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 sportowych 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 ekspertami kataklizmów. Rola intensywna w fazie treningów, później w trybie utrzymania.

9.3.9 Data Engineers

Data Engineerzy 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 testerzam z przetestowaniem frontu.

9.3.12 Eksperci Kataklizmów

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 Prawnicy

Prawnicy wspierają Głównego Prawnika, przygotowują opinie oraz analizują zgodność przetwarzania danych z przepisami lokalnymi i unijnymi. Uczestniczą w tworzeniu regulaminów, polityk prywatności i umów integracyjnych. Pracują w zależności od potrzeb projektu i zmian regulacyjnych.

9.3.14 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.

9.3.15 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 TRL. 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.