

# Podsumowanie projektu FRED-T

Wykrywanie anomalii  
i nadużyć telekomunikacyjnych  
oraz zbadanie możliwości identyfikacji zagrożeń  
w czasie rzeczywistym

Nr WKP 1/1.4.1/1/2006/87/87/642/2007/U



## Spis treści:

1.	KONCEPCJA I MISJA PROJEKTU.....	3
2.	PODMIOTY ZAANGAŻOWANE W REALIZACJĘ PROJEKTU .....	4
3.	WSKAZANIE PODSTAW TECHNICZNYCH I TECHNOLOGICZNYCH.....	4
4.	HARMONOGRAM PRZEPROWADZONYCH PRAC .....	9
5.	OPIS WDROŻONYCH BADAŃ.....	10
6.	OMÓWIENIE POWSTAŁEGO PROTOTYPU .....	10
7.	WYNIKI PRZEPROWADZONYCH BADAŃ .....	11
8.	ANALIZA I WNIOSKI KOŃCOWE .....	13



# 1. Koncepcja i misja projektu

## Koncepcja projektu

Działania realizowane w ramach projektu celowego są zgodne z wytycznymi UE „Community framework for state aid for research and development” i ukierunkowane na pozyskanie wiedzy, która może być wykorzystana w rozwoju nowych rozwiązań, procesów czy usług.

Projekt wpisuje się w cele określone w dokumentach strategicznych na poziomie Unii Europejskiej:

- Polityka Rozwoju Społeczeństwa Informacyjnego - Podejmowane działania badawczo-rozwojowe służą rozwojowi społeczeństwa informacyjnego poprzez rozbudowę regionalnej infrastruktury badawczej w dziedzinie ICT oraz wyrównanie dysproporcji pomiędzy regionami Polski i UE w zakresie wykorzystania nowoczesnych technologii telekomunikacyjnych i teleinformatycznych
- Strategia Lizbońska - Wyrazem coraz głębszego powiązania między badaniami naukowymi, a rozwojem gospodarki jest dążenie każdego państwa UE do osiągnięcia poziomu wydatków na B+R, który będzie stanowił 3% PKB. Tymczasem sektor o najwyższym stopniu innowacyjności to sektor prywatny
- Strategia zwiększenia nakładów na działalność B+R w celu osiągnięcia założeń Strategii Lizbońskiej - projekt badawczy był finansowany zarówno ze środków publicznych jak i środków własnych Wnioskodawcy.
- Szósty Program Ramowy Badań i Rozwoju Technicznego (2002-2006) - obszarem wspólnym 6PR Rozwoju Technicznego i omawianego projektu jest budowa społeczeństwa informacyjnego i badania prowadzone w ramach Priorytetu - Technologie Społeczeństwa Informacyjnego (*Information Society Technologies- IST*).

oraz kraju:

- Narodowy Program Rozwoju na lata 2004-2006 - Projekt mieści się w podstawowym założeniu NPR, jakim jest poprawa pozycji konkurencyjnej przedsiębiorstw działających na terenie Polski w warunkach Jednolitego Rynku Europejskiego
- Sektorowy Program Operacyjny – Wzrost Konkurencyjności Przedsiębiorstw na lata 2004-2006 – projekt realizuje założenia SPO-WKP wpisując się w NPR 2004-2006 w zakresie poprawy pozycji konkurencyjnej przedsiębiorstw działających w kraju
- ePolska – Plan działań na rzecz rozwoju społeczeństwa informacyjnego w Polsce na lata 2001-2006 - projekt realizuje cele strategii ePolska:  
Cel 1: Powszechny, tańszy, szybszy i bezpieczny Internet - Bezpieczeństwo sieci  
Cel 3: Stymulowanie lepszego wykorzystania technologii informacyjnych - Gospodarka elektroniczna
- Strategia kierunkowa rozwoju informatyzacji Polski do roku 2013 oraz perspektywiczna prognoza transformacji społeczeństwa informacyjnego do roku 2020
- Proponowane kierunki rozwoju nauki i technologii w Polsce do 2020 r. - projekt bezpośrednio wpisuje się w następujące strategiczne obszary badań naukowych wspomagających rozwój technologii informatycznych/informacyjnych i związanej z nimi informatyzacji kraju

Projekt znajduje korelację w programach regionalnych tworzonych dla regionów: mazowieckiego i śląskiego (z racji lokalizacji oddziałów ABG)

## Misja projektu

Wzmocnienie potencjału i rozwój społeczeństwa informacyjnego poprzez zdobycie nowej wiedzy przy wytworzeniu udoskonalenia istniejącego rozwiązania organizacyjno-technicznego.

## 2. Podmioty zaangażowane w realizację projektu

- Asseco Poland SA – obecny Beneficjent umowy z MNiSW pierwotnie umowa z MNiSW została przez firmę SPIN SA, umowa była kontynuowana przez ABG SA następcę prawnego SPIN SA, od 1 10.2008 następcą prawnym ABG SA stało się Asseco Poland SA
- POSTINFO SP. z o.o. – realizator projektu, uczestnik konsorcjum z ABG
- Instytut Innowacji i Społeczeństwa Informatycznego Sp. z o.o. – wykonawca zadań badawczych oraz wsparcie sprawozdawczości i rozliczeń z MNiSW
- Politechnika Warszawska – Wydział Elektryczny Instytut Sterowania i Elektroniki Przemysłowej – wykonawca prac badawczych

## 3. Wskazanie podstaw technicznych i technologicznych

### Potrzeba projektowania systemów automatycznego odwzorowania i korelowania zdarzeń biznesowych (SAB).

Obecnie powszechnie przyjętym celem projektowania i budowania systemów jest taki sposób implementacji poprzez integrację gotowych komponentów lub produkcji nowych elementów, w wyniku którego osiąga się spełnienie wszystkich celów strategicznych, wszystkich potrzeb użytkowników, itd.

W praktyce okazuje się, że potrzeby, warunki techniczne, oczekiwana funkcjonalność zmieniają się „z dnia na dzień” i często się zdarza, że zbudowany wielkim wysiłkiem system organizacyjno-techniczny chwilę po jego implementacji nie spełnia już obecnych potrzeb organizacji, w której funkcjonuje i nie odwzorowuje właściwie procesów biznesowych, które obsługują jej działalność.

Często okazuje się zadaniem zbyt złożonym i zbyt czasochłonnym, aby obserwować wszelkie procesy biznesowe i remodelować „na gorąco” i „ręcznie” system organizacyjno-techniczny pod kątem pełnego odzwierciedlenia zmienionych procesów, zdarzeń i danych.

Ambitnym celem zaprojektowania i budowy systemów automatycznego odwzorowania i korelowania zdarzeń biznesowych jest przełamanie ww. barier rozwoju biznesu, czy usług społecznych na poziomie organizacyjno-technicznym poprzez stworzenie środowiska „sztucznej inteligencji”, które wykona odpowiednie „dostosowanie” przetwarzania zdarzeń i danych do zmienionej charakterystyki procesów biznesowych, jak i potrzeb użytkowników.

Co najważniejsze, te automatyczne systemy nie zawierają automatyki, lecz wykorzystują zintegrowany dorobek nauki w dziedzinie sztucznej inteligencji (SI) z obszarów:

- systemy ekspertowe,
- algorytmy ewolucyjne,
- logika rozmyta,
- sztuczne sieci neuronowe.

### Podstawowe założenia dla architektury zewnętrznej

#### 1. Standaryzacja interfejsów (nie komponentów):

- powinny mieć taką samą definicję,
- używanie meta-języka wszędzie tam, gdzie tylko jest to możliwe (XML, WSDL),
- celem jest możliwość realizacji idei podłączania modułów w trybie „plug-and-play” i ich szybkiej integracji.

#### 2. Middleware:

- zapewnia bazujące na wymianie komunikatów – tzw. szynę komunikacyjną oraz usługi integracyjne,
- publikuje/pobiera w trybie punkt-w-punkt, zapewnia transport komunikatów na poziomie cech systemu plików,
- zapewnia łatwość dodawania nowych narzędzi, wzmacnia efekt dodany integracji.

### 3. Wybór użytkownika:

- nie istnieją ograniczenia w zakresie wyboru komponentów, o ile spełniają wymogi interfejsów,
- użytkownik poprzez narzędzie modelowania przepływu procesów biznesowych ma możliwość dynamicznej zmiany modelu i funkcjonalności systemu jako całości.

Dane i zdarzenia występujące w tym środowisku są opisane w modelu obiektowym (Klasa Zdarzenia, Czas, Monitorowanie, Zasoby) i generują komunikaty przetwarzane na wspólnej szynie integracyjnej (Middleware) w funkcjonalnościach określonych przez moduły systemowe środowiska.

Głównym założeniem modelowej architektury systemu jest lokalizacja SAB w środowisku zewnętrznym zgodnym z przedstawionym w poprzednim punkcie modelem. Przyjmuje się, że funkcjonalność kanałów detekcji przejmuje wspomniana szyna komunikacyjna wraz z usługami integracyjnymi, które odpowiadają w takim schemacie za funkcjonalność obsługi interfejsów odwzorowywanych systemów trzecich.

Modelowa architektura opiera się na metodzie PSM (ang. *Problem-Solving-Method*), opisanej poniżej.

### Zastosowanie metody PSM w modelowej architekturze

Metoda ta wprowadza wielowarstwowość analizy problemu w oparciu o metody niższego rzędu, których użycie realizuje podzadanie danego zadania i skorelowaną analizę wyników podzadań poprzez użycie metody wyższego rzędu.

Oczywiście stosowane metody PSM to opisane matematycznie narzędzia, takie jak:

- logika konwencjonalna,
- rozumowanie autoepistyczne,
- logika domysłów,
- metoda oparta na regułach (np. wektory wiedzy),
- sieci semantyczne,
- heurystyki, itd.

Realizacja metod PSM opiera się na bazie wiedzy, istotnym elementem architektury rozwiązania jest więc podsystem pozyskiwania wiedzy i samoczenia się.

### Mapowanie celów niniejszego projektu w odniesieniu do w/w standardów oraz najlepszych w skali świata lub krajów Unii Europejskiej rozwiązań

Przyjmując nomenklaturę zdefiniowaną prezentowanymi powyżej modelami (standardy światowe), dokonujemy mapowania celów niniejszego projektu:

- Środowisko odwzorowywane – systemy rozliczeń i usług abonenckich operatorów telekomunikacyjnych.
- Interfejsy do środowiska – lokalne systemy obsługi klienta tych operatorów, związane z realizacją usług dla klientów.
- Kanały danych – adaptory do interfejsów wykonane zgodnie z wymaganiami szyny komunikacyjnej.
- Szyna komunikacyjna – szyna komunikacyjna operatora.
- System SAB – znaczące udoskonalenie rozwiązania w odniesieniu do ww. elementów mapowania.
- Metody PSM – przetwarzanie regułowe.
- Narzędzie Domain Tool – zamodelowane i zaprototypowane nowe narzędzie w odniesieniu do ww. elementów mapowania.

### **Opis instalacji doświadczalnej, prototypu doświadczalnego nowo zaprojektowanego wyrobu**

Udoskonalenie oznacza znaczącą modyfikację istniejącego rozwiązania organizacyjno-technicznego zamodelowanego wskutek niniejszego projektu w etapie badań przemysłowych.

Udoskonalenie w szczególności oznacza:

1. Wykonanie planowych i wspólnych badań przez Wnioskodawcę przy udziale Środowiska Wdrożenia oraz Doradcy w zakresie dotyczącym misji projektu.
2. Przekształcenie wyniku tych badań w model oraz realizację Udoskonalenia istniejącego rozwiązania; nie będą obejmowały swym zasięgiem rutynowych, czy też okresowych zmian dotychczasowych rozwiązań Wnioskodawcy, nie będą zawierały też innych działań o charakterze ulepszającym ale nie związanych bezpośrednio z procesami badawczymi.
3. Przeprowadzenie w Środowisku Wdrożenia testów akceptacyjnych bezpośrednich, jak i przekształconych wyników badań nad Udoskonaleniem, wdrożenie rozwiązania jako całości oraz kontrola przydatności technicznej i ekonomicznej.

Udoskonalenie stanowiące przedmiot projektu „Wykrywanie anomalii i nadużyć telekomunikacyjnych oraz zbadanie możliwości identyfikacji zagrożeń w czasie rzeczywistym” w szczególności zawiera:

- model procesów biznesowych występujących podczas realizacji w strukturach organizacyjnych podobnych do Środowiska Wdrożenia
- model procesów biznesowych występujących podczas komunikacji w strukturach organizacyjnych podobnych do Środowiska Wdrożenia
- księgę procedur realizujących procesy biznesowe
- projekt zasad polityki bezpieczeństwa dla realizowanych w przyszłości na bazie udoskonalenia rozwiązań komercyjnych
- projekt architektury, warstw i komponentów dla realizowanych w przyszłości na bazie udoskonalenia rozwiązań komercyjnych
- określenie parametrów technicznych dla realizowanych w przyszłości na bazie udoskonalenia rozwiązań komercyjnych
- propozycje wyboru tych cech technicznych, które mogą być standardami technicznymi dla realizowanych w przyszłości na bazie Udoskonalenia rozwiązań komercyjnych
- projekt oraz dostarczenie niezbędnej aparatury badawczej celem wdrożenia w Środowisku Wdrożenia
- udoskonalenie kodu aplikacji informatycznej celem osiągnięcia podstawowej funkcjonalności testowej zgodnej z przyjętymi modelami danych, księgami procedur i zasadami, polityki bezpieczeństwa
- wykorzystanie Środowiska Wdrożenia do testów akceptacyjnych dla obsługi udoskonalonego rozwiązania oraz pomiaru TCO

Zakres Udoskonalenia obejmuje:

- rozbudowę mechanizmów czasu rzeczywistego (m.in. wykorzystanie danych z systemu sygnalizacji międzycentralowej SS7, co pozwoliłoby na reagowanie w określonych przypadkach już podczas inicjowania połączenia lub w jego trakcie)
- dodanie do rozwiązania wewnętrznego podsystemu obiegu informacji z możliwością jego integracji z systemami operatora
- rozbudowa metod analizy opartych o zidentyfikowane przypadki nieprawidłowości (fingerprinting)
- wprowadzenie rozwiązań typu GRID
- wprowadzenie warstwy middleware'u do komunikacji z innymi aplikacjami zgodnie ze standardami NGOSS-OSS/J

### **Funkcjonalność obecna SAB**

Przeznaczeniem systemu FRED jest wykrywanie nadużyć w sieciach telefonicznych. Z uwagi na to, że system ten nie spełniał wszystkich wymagań, jakie były przed nim stawiane, dlatego Wnioskodawca zamierzył go udoskonalić. Zaimplementowane w systemie elastyczne mechanizmy analizy danych, oprócz wykrywania błędów i nadużyć, mogą być z powodzeniem wykorzystywane do wspomagania procesów ochrony przychodów, sprzedaży, marketingu oraz ochrony kluczowych klientów.

System FRED może przyjmować różnego rodzaju dane z różnych źródeł. Mogą to być pliki z rekordami bilingowymi dostarczane przez systemy mediacji lub dane ruchowe w różnej postaci dostarczane bezpośrednio z central, z systemu zarządzania sygnalizacją SS7 lub z systemów zarządzania innymi typami sygnalizacji w czasie rzeczywistym. Dostarczane do systemu informacje są przetwarzane i mogą być przechowywane w bazie danych lub w plikach binarnych.

System agreguje otrzymywane informacje. W skład agregatów wchodzi przede wszystkim profile, które mogą być tworzone dla każdego numeru konta, dla każdego numeru klienta (dla potrzeb analizy ruchu abonenckiego) oraz dla każdej wiązki, grupy wiązek, operatora (dla potrzeb analizy ruchu międzyoperatorskiego). System wykonuje automatycznie wielokryterialną analizę zagregowanych informacji. Analiza wykonywana jest z ustaloną przez użytkownika częstotliwością.

System został również wyposażony w moduł regulowy, którego elastyczne mechanizmy pozwalają na konstruowanie złożonych zapytań i sprawdzanie ich na dostępnych w systemie danych. Informacje o wykrytych zdarzeniach mogą być udostępniane użytkownikom systemu za pomocą poczty elektronicznej, poprzez interfejs WWW lub w postaci plików w różnych formatach (np. \*.html, \*.csv, \*.txt).

Moduł zarządzania użytkownikami systemu umożliwia tworzenie różnych profili użytkowników w zależności od aktualnych potrzeb, zarówno jeśli chodzi o dostęp do systemu, jak i otrzymywane raporty.

System wykonuje następujące rodzaje analiz:

- Analizę Ruchu Abonenckiego – przeznaczoną do wykrywania nadużyć, zarówno o znanym (system regulowy), jak i nieznanym charakterze (analiza zmian zachowania abonentów) oraz do monitorowania i ochrony kluczowych klientów
- Analizę Ruchu Międzyoperatorskiego – przeznaczoną do wykrywania i alarmowania zmian w ruchu przychodzącym od innych operatorów i wychodzącym do innych operatorów, bilansowania ruchu, wykrywania tras połączeń przynoszących zysk poniżej ustalonej wartości progowej (stratę). Analiza obejmuje:
  - wykrywanie i alarmowanie tras połączeń generujących zysk mniejszy od zadanej wartości progowej na podstawie analizy danych ruchowych oraz aktualnych stawek rozliczeń międzyoperatorskich
  - wykrywanie i alarmowanie w przypadku stwierdzenia istotnych zmian w strukturze ruchu – agregacja danych ruchowych względem wiązek oraz okresowa analiza zachodzących zmian w strukturze ruchu
  - bilansowanie ruchu przychodzącego do sieci i wychodzącego z sieci poprzez agregowanie na poziomie operatorów, wiązek i frakcji ruchu
  - wykrywanie błędów i nadużyć związanych z rozliczeniami międzyoperatorskimi
  - Kontrolę Poprawności Przetwarzania Systemu Bilingowego – przeznaczoną do wykrywania błędów i nadużyć oraz sprawdzania kompletności danych w czasie przetwarzania ich przez system bilingowy, a także do kontroli poprawności rozliczania abonentów (mechanizmów taryfikacji) – retaryfikacja bilingu losowo wybranych abonentów w celu kontroli poprawności wystawionych faktur, według zasad, taryf, reguł rozliczania dostarczonych przez operatora
  - Kontrolę Poprawności Przetwarzania Systemu Interconnect – przeznaczoną do wykrywania błędów i nadużyć oraz sprawdzania kompletności danych w czasie przetwarzania ich przez system Interconnect, a także do kontroli poprawności rozliczeń międzyoperatorskich
  - kontrolę poprawności procesu rozliczeń międzyoperatorskich
  - badanie kompletności i poprawności (procesu) przetwarzania danych na poziomie wiązek, operatorów oraz frakcji

Za import danych do systemu odpowiedzialny jest Agent, czyli oprogramowanie skojarzone ze źródłem danych, umieszczone jak najbliżej tego źródła, które spełnia następujące funkcje:

- pobieranie danych z różnych źródeł w formacie i w sposób właściwy dla tego źródła
- standaryzacja rekordów
- wstępna analiza danych, np. wykrywanie alarmów gorących

- agregacja danych
- dystrybucja wykrytych alarmów zgodnie z ustawieniami użytkowników:
  - na ekran analityka
  - do bazy danych
  - przesyłanie informacji, np. za pomocą poczty elektronicznej do odpowiednich komórek w celu podjęcia dalszych kroków
  - automatyczne generowanie zadań w systemach klienta

Dane do systemu mogą pochodzić z wielu źródeł:

- system sygnalizacji (SS7)
- centrale
- systemy mediacji
- systemy bilingowe
- inne systemy informatyczne (VoIP, VM, CRM)

Równoczesne pobieranie informacji z kilku źródeł pozwala na przeprowadzanie analizy porównawczej, a tym samym kontrolę kompletności danych bilingowych na poszczególnych etapach przetwarzania.

W zależności od potrzeb analizy, gromadzone w systemie FRED® dane mogą być agregowane na różne sposoby:

- dla poszczególnych linii telefonicznych
- dla poszczególnych klientów (łączenie danych dla wszystkich linii danego klienta)
- dla poszczególnych grup klientów (np. analizy klas abonentów)
- dla poszczególnych wiązek, grup wiązek, operatorów (analiza ruchu międzyoperatorskiego)
- agregacja według poszczególnych stref numeracyjnych
- agregacja według central

Architektura systemu składa się z następujących podstawowych znaczników:

- platforma: Unix – Sun Solaris lub Microsoft Windows Server 2003
- wykorzystane języki programowania: C++, Java, SQL, Matlab (w celu efektywnego wykorzystania skomplikowanych funkcji matematycznych na etapie przetwarzania danych)
- baza danych Oracle® (zapewnia odpowiedni poziom bezpieczeństwa: autoryzacja użytkowników, przechowywanych danych osobowych)
- współpraca z zewnętrznymi aplikacjami (np. i2, Matlab, Statistica, itp.)
- skalowalność (prawie liniowa zależność szybkości przetwarzania systemu od mocy obliczeniowej)

W poniższej tabeli dokonano zestawienia wady i zalety istniejących na rynku systemów.

Lp.	Wady istniejących rozwiązań	Zalety istniejących rozwiązań
1	Brak narzędzi i analiz wykrywania anomalii, błędów oraz nadużyć w sieciach telekomunikacyjnych.	Rozwiązania kompleksowe wielomodułowe zachodnich producentów.
2	Brak elastycznych rozwiązań wprowadzania i analizowania reguł w sieciach telekomunikacyjnych.	
3	Brak analiz profilowych abonenta (obserwacja w czasie rzeczywistym i uruchamianie alarmów).	
4	Istniejące rozwiązania bazują na dużych bazach danych i występuje w nich problem wydajności przetwarzania danych.	
5	Wysokie koszty eksploatacji, rozwoju i serwisu.	
6	Długie czasy reakcji i realizacji producentów istniejących rozwiązań.	
7	Brak lokalizacji do warunków rynku polskiego.	

Źródło: Opracowanie własne Wnioskodawcy

#### 4. Harmonogram przeprowadzonych prac

Lp	Nr i tytuł zadania	Wykonawca zadania	Termin rozpoczęcia	Termin zakończenia
<b>Badania przemysłowe</b>				
1	Zadanie 1 – Badania i opracowanie modeli rdzenia systemu	ABG, POSTINFO, INSI	05-2007	09-2007
2	Zadanie 2 – Badania i opracowanie modelu danych i przetwarzania w systemie	ABG, POSTINFO, INSI	05-2007	09-2007
3	Zadanie 3 – Badania i opracowanie modeli interfejsów użytkowych pod kątem ich późniejszego prototypowania	ABG, POSTINFO, INSI	05-2007	09-2007
4	Zadanie 4 – Opracowanie modeli modułów systemu pod kątem ich późniejszego prototypowania	ABG, POSTINFO, INSI	10-2007	12-2007
<b>Badania przedkonkurencyjne</b>				
5	Zadanie 5 – Wytworzenie prototypu nowego systemu opartego na znaczącym udoskonaleniu istniejącego systemu FRED oraz kilka iteracji typu “test-poprawki”, aż do osiągnięcia wersji stabilnej systemu	ABG, POSTINFO, INSI, ISEP	01-2008	05-2008
<b>Prace wdrożeniowo-inwestycyjne</b>				
6	Zadanie 6 – Przygotowanie wdrożenia	ABG, POSTINFO	06-2008	07-2008
7	Zadanie 7 – Instalacja i wdrożenie serii próbnej rozwiązania	ABG, POSTINFO, SFERIA	06-2008	07-2008
8	Zadanie 8 – Odbiór wdrożenia pilotażowego	ABG, POSTINFO	06-2008	07-2008

## 5. Opis wdrożonych badań

Badania przemysłowe – miały na celu wyjaśnienie czy teoretyczne rozwiązanie misji projektu jest możliwe do zastosowania zarówno ze względów technicznych, jak i ekonomicznych. W ramach badań opracowano modele rdzenia systemu, danych, przetwarzania, interfejsów.

Badania przedkonkurencyjne – miały na celu stworzenie prototypu, który nie będzie przekształcony ani wykorzystany w sposób bezpośredni do zastosowania przemysłowego czy handlowego. Modelowy prototyp rozwiązania technicznego został przetestowany w środowisku produkcyjnym operatora telekomunikacyjnego. Celem testowania było uzyskanie oceny możliwości zastosowania w praktyce – testy akceptacyjne.

## 6. Omówienie powstałego prototypu

W wyniku prowadzonych prac w ramach projektu "Wykrywanie anomalii i nadużyć telekomunikacyjnych oraz zbadanie możliwości identyfikacji zagrożeń w czasie rzeczywistym", powstał prototyp systemu FRED-T, jako udoskonalenie systemu FRED 5.188.

W ramach prototypu, zgodnie z przyjętymi przez Wnioskodawców założeniami, w systemie zaimplementowane zostały nowe moduły:

- FRED-T.Analizator\_fingerprinting,
- FRED-T.Analizator\_profilu,
- FRED-T.Analizator\_SS7,
- FRED-T.Grid,
- FRED-T.Komunikator,
- FRED-T.Rdzen.

Prototyp systemu został wdrożony w środowisku testowym u operatora telekomunikacyjnego SFERIA S.A. Umożliwiło to przeprowadzenie szczegółowych testów w oparciu o zestaw danych rzeczywistych, udostępnionych przez operatora. Testy prowadzono w okresie 2 miesięcy, a udostępnione dane obejmowały okres 6 miesięcy 2008 co umożliwiało przeprowadzenie zarówno testów wydajnościowych jak i testów poprawności opracowanych mechanizmów m.in. związanych z predykcją, które do poprawnego działania wymagają pewnej historii aktywności danego konta/numeru.

Funkcjonalność poszczególnych modułów prototypu zmodyfikowano w trakcie testów w celu dostosowania do przyjętej metodyki testowania modułu i usunięcia wykrytych w trakcie testów błędów. Przeprowadzone testy pozwalają na stwierdzenie, że przyjęte założenie i rozwiązania spełniają postawione wymagania projektowe i umożliwiają realizację założonej funkcjonalności. Zatem można oczekiwać, iż opracowane moduły wzbogacą w przyszłości funkcjonalność wersji produkcyjnej systemu FRED-T.

## 7. Wyniki przeprowadzonych badań

Realizacja projektu obejmowała następujące prace badawczo-rozwojowe:

### Zadanie 1 "Badania i opracowanie modeli rdzenia systemu"

Zadanie pierwsze realizowane było dwutorowo. W ramach tego zadania dokonano analizy dotychczasowych rozwiązań architektonicznych przyjętych w systemie FRED w celu ustalenia tych, które sprawdziły się w tymże systemie w praktyce i wyeliminowania problemów wykrytych w starej architekturze, w miejsce których opracowano nowe rozwiązania. Drugim obszarem prac w zadaniu było poszukiwanie optymalnego rozwiązania do przyszłej implementacji mechanizmu reguł, takiego by z jednej strony dać dużą elastyczność i wygodę użytkownikowi, a z drugiej strony zapewnić maksymalną wydajność rozwiązania. Przeanalizowano mechanizmy stworzone w systemach FRED i SPINRULES i na tej podstawie opracowano założenia do nowego modelu mechanizmu reguł dla nie komercyjnego prototypu FRED-T.

W ramach zadania pierwszego powstały następujące opracowania:

1. Opis metod rozliczeń oraz symulacyjne badanie ich skuteczności, w czasie rzeczywistym, na bazie populacji danych badawczych
2. Optymalizacja schematów procesów biznesowych pod kątem systemu przychodów typowego alternatywnego (konkurującego z TP S.A.) operatora telekomunikacyjnego
3. Opracowanie badawcze nt. skuteczności mechanizmu reguł biznesowych na bazie symulacji zdarzeń procesów biznesowych badanego operatora telekomunikacyjnego
4. Opracowanie optymalnego modelu architektury systemu i modelu platformy integracyjnej

### Zadanie 2 „Badania i opracowanie modelu danych i przetwarzanie w systemie”

Prace realizowane w ramach zadania drugiego skoncentrowane były na badaniu możliwości wykorzystania istniejących elementów systemu FRED do budowy rozwiązania z opcją integracji poprzez platformę integracyjną. Drugim istotnym obszarem badań były poszukiwania bardziej uniwersalnych, a jednocześnie zapewniających szybsze działanie modeli danych i modeli przetwarzania.

Efektom tych prac są następujące opracowania:

1. Analiza efektywności wybranych standardów wykorzystywanej platformy integracyjnej w celu optymalizacji komunikacji wewnętrznej i zewnętrznej systemu, na bazie symulacji standardowych interfejsów dla populacji alternatywnych operatorów telekomunikacyjnych
2. Analiza koncepcji silnika taryfikacyjnego w celu poprawy jego efektywności poprzez optymalizację mechanizmu reguł, na bazie symulacji procesów biznesowych standardowych dla populacji alternatywnych operatorów telekomunikacyjnych
3. Opracowanie modelu danych i przetwarzania

### Zadanie 3 „Badania i opracowanie modeli interfejsów użytkowych pod kątem ich późniejszego prototypowania”

W zadaniu trzecim badano różne podejścia do interfejsu użytkownika, w celu opracowania rozwiązania umożliwiającego lepszą prezentację danych oraz większą wygodę takiego, które pozwoliłoby zwiększyć dostępność nie komercyjnego prototypu FRED-T bez zmniejszenia wygody użytkownika. Po analizie rozwiązania przyjętego w systemie FRED, zdecydowano się na odejście od interfejsu użytkownika w części opartej o aplikację lokalną stosowaną w tym systemie i zastąpienie jej interfejsem użytkownika dostępnym z poziomu przeglądarki WWW. W ramach ostatniego punktu udało się między innymi opracować architekturę oraz projekt modułu pomocy kontekstowej, który planuje się wykorzystać jako element powstających w kolejnych etapach interfejsów użytkownika.

W wyniku zadania trzeciego powstały następujące opracowania:

1. Opracowanie optymalnego modelu autodefinicji procesów biznesowych przez typowego użytkownika alternatywnego operatora telekomunikacyjnego z wykorzystaniem wniosków z badań optymalizacji mechanizmu reguł

2. Analiza efektywności udoskonalanego modułu Konfiguratora Produktów powiązanego z algorytmami wyceny i silnikiem taryfikacyjnym w optymalizacji schematów procesów biznesowych w systemie przychodów typowego alternatywnego operatora telekomunikacyjnego
3. Badanie i opracowanie modeli interfejsów.

#### **Zadanie 4 „Opracowanie modeli modułów systemu pod kątem ich późniejszego prototypowania”**

W zadaniu czwartym zespół skupił się na zagadnieniach pozwalających przyspieszyć wykrywanie nieprawidłowości. Ponadto prowadzono także dalsze prace nad mechanizmami reguł, a także powstał projekt modelu modułu Konfiguratora Produktów powiązanego z algorytmami wyceny i silnikiem taryfikacyjnym.

Podczas realizacji zadania czwartego powstały następujące opracowania:

1. Opracowanie optymalnego modelu modułów mechanizmów realizujących operacje rozliczeniowe w czasie rzeczywistym
2. Opracowanie optymalnego modelu silnika taryfikacyjnego działającego w oparciu o mechanizm reguł
3. Opracowanie udoskonalonego modelu modułu Konfiguratora Produktów powiązanego z algorytmami wyceny i silnikiem taryfikacyjnym w procesie optymalizacji przychodów operatora telekomunikacyjnego

#### **Zadanie 5 „Wytworzenie niekomercyjnego prototypu nowego systemu opartego na znaczącym udoskonaleniu istniejącego systemu FRED oraz kilka iteracji typu „test-poprawki”, aż do osiągnięcia wersji stabilnej systemu.”**

W ramach prowadzonych badań przedkonkurencyjnych powstał niekomercyjny prototyp, który umożliwił zbadanie przydatności i skuteczności opracowanych algorytmów i modeli w wykrywaniu nadużyć oraz nieprawidłowości w obszarze telekomunikacyjnym. Wykorzystano sygnalizację SS-7 jako dodatkowe źródło danych do analizy. W ramach projektu, podwykonawca konsorcjum - Instytut Sterowania i Elektroniki Przemysłowej Politechniki Warszawskiej - opracował algorytmy wykrywania nadużyć, które zostały zaimplementowane w przedmiotowym systemie (m. in. fingerprinting oraz analiza profili abonentów, pod kątem występujących anomalii). Przetestowane zostały także możliwości budowy uniwersalnych mechanizmów komunikacji systemu z innymi systemami u operatora telekomunikacyjnego poprzez budowę mechanizmu komunikacji z systemami obiegu informacji. Zbadano również przydatność rozwiązań typu GRID do równoległego prowadzenia części obliczeń w celu uzyskania większej szybkości przetwarzania danych i skrócenia czasu wykrywania nieprawidłowości.

W ramach zadania piątego powstały następujące niekomercyjne moduły prototypowe:

1. Prototyp modułu rozwiązania rdzenia-platformy technologicznej pod potrzeby architektury modułowej
2. Prototyp modułu analizującego dane z sygnalizacji SS-7
3. Prototyp modułu analiz typu fingerprinting
4. Prototyp modułu komunikacji z systemami obiegu informacji
5. Prototyp modułu analizy profili abonentów, pod kątem występujących anomalii
6. Prototyp klastra GRID

**Prace wdrożeniowe zrealizowane w ramach projektu obejmują następujące zadania:**

**Zadanie 6 „Przygotowanie wdrożenia”,**

**Zadanie 7 „Instalacja i wdrożenie serii próbnej rozwiązania”,**

**Zadanie 8 „Odbiór wdrożenia pilotażowego”.**

Niekomercyjny prototyp systemu FRED-T powstały w efekcie przeprowadzonych prac badawczych, został uruchomiony w środowisku produkcyjnym operatora telekomunikacyjnego - firmy SFERIA SA. Przeprowadzone testy potwierdzają, że otrzymane w wyniku prac badawczych rozwiązania sprawdzają się i będzie możliwe ich dalsze wykorzystanie w produkcie komercyjnym, który powstanie na bazie uzyskanego prototypu niekomercyjnego.

## 8. Analiza i wnioski końcowe

### Zakres Udoskonalenia

Zgłoszony do realizacji projekt zawarł następujące działania służące poprawieniu i unowocześnieniu systemu FRED®:

- rozbudowę mechanizmów czasu rzeczywistego – dzięki temu rozwiązaniu zaistnieje możliwość wykorzystania danych z systemu sygnalizacji międzycentralowej SS7, co pozwoli na reagowanie w określonych przypadkach już podczas inicjowania połączenia lub w jego trakcie
- dodanie do rozwiązania wewnętrznego podsystemu obiegu informacji z możliwością jego integracji z systemami operatora
- rozbudowę metod analizy opartych o zidentyfikowane przypadki nieprawidłowości (fingerprinting)
- wprowadzenie rozwiązań typu GRID
- wprowadzenie warstwy middleware do komunikacji z innymi aplikacjami zgodnie ze standardami NGOSS-OSS/J

### Elementy badawcze i innowacyjne

Realizacja projektu doprowadziła do wykorzystania elementów innowacyjnych opracowanych w wyniku przeprowadzenia prac badawczo-rozwojowych. Dotychczasowe rozwiązania dotyczące systemów wykrywania włamań i nadużyć telekomunikacyjnych są rozwiązaniami wielomodułowymi, pochodzącymi od producentów z Europy Zachodniej. Rozwiązania te posiadają wiele wad, wśród których można wymienić:

- wysokie koszty eksploatacji, developmentu (rozwoju) i serwisowania
- długie czasy reakcji i produkcji rozwiązania
- brak przystosowania systemów do warunków rynku polskiego

Wnioskodawca poprzez realizację niniejszego projektu wykorzystał istniejącą lukę rynkową. Projekt został realizowany przy wykorzystaniu metod, które dotychczas nie były stosowane w tej dziedzinie. Innowacje polegają na:

- zastosowaniu zaawansowanych algorytmów matematycznych dekompozycji na wartości singularne macierzy (Singular Value Decomposition – SVD) w rozwiązaniach telekomunikacyjnych; pozwoliło to na zwiększenie możliwości przetwarzania i analizy zjawisk zachodzących w sieciach telekomunikacyjnych oraz w znaczący sposób poprawiło przetwarzanie danych w sieciach telekomunikacyjnych przy jednoczesnym znaczącym obniżeniu kosztów rozwiązania
- zastosowaniu po raz pierwszy na rynku narzędzia do wykrywania i analiz anomalii, błędów i nadużyć w sieciach telekomunikacyjnych
- zastosowaniu po raz pierwszy na rynku możliwości elastycznego definiowania profili abonentów oraz analizy wielowymiarowej zmian w czasie rzeczywistym tych profili w wyniku działalności abonenta lub osoby trzeciej
- zastosowaniu po raz pierwszy na rynku możliwości definiowania reguł i analizy tych reguł w systemach telekomunikacyjnych (do tego celu będzie wykorzystywane prosty interfejs graficzny GUI)
- dostosowaniu rozwiązania do warunków polskich

Zaletami systemu, jaki powstał w wyniku realizacji projektu, są atrakcyjne ceny zakupu, wdrożenia, szkolenia, utrzymania, rozbudowy i serwisowania. System zapewnia ochronę interesów operatora telekomunikacyjnego, jak również ochronę jego klientów. Umożliwia szybką reakcję w przypadku pojawienia się prób kradzieży lub nadużyć. Stanowi nową jakość w budowaniu zaufania i lojalności klienta do operatora, umacniając jego pozycję rynkową.