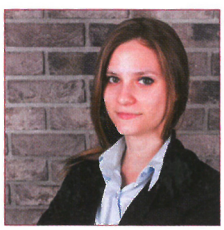
# Inżynieria odwrotna – hardware, software i praktyka

**Jako osoba łącząca ze sobą trzy techniczne światy – inżynierię oprogramowania, optymalizację produkcji i inżynierię biomedyczną – miałam w czasie swojej dotychczasowej aktywności zawodowej okazję obserwować różne przejawy wykorzystania inżynierii odwrotnej na mniej albo bardziej zaawansowanym poziomie, a także przy motywacji gorszymi bądź lepszymi intencjami.**



mgr inż. Agnieszka Hyla
Quality assurance engineer w 314 Apps Ltd., konsultantka ds. optymalizacji produkcji w EMT-Systems sp. z o.o., doktorantka Politechniki Śląskiej, Wydziału Inżynierii Biomedycznej.

Inżynieria odwrotna to ogólnie zbiór metod i sposobów działania pozwalających na poznanie działania danego obiektu. Obiektem tym może być implant medyczny, proteza, zaawansowana technologicznie maszyna czy kod programistyczny. W zależności od typu i poziomu skomplikowania obiektu wykorzystujemy inne metody, wynik jest jednak jeden – opracowanie pierwotnego sposobu wytworzenia elementu, tak by w następnym kroku można było ten obiekt powielić lub zmodyfikować.

## INŻYNIERIA WSTECZNA W ODZWIERCIEDLANIU PROCESÓW

Trzon produkcji i wytwarzania stanowią procesy, czyli powtarzalne schematy postępowania, które prowadzą do określonych w przybliżeniu efektów. W zależności od jakości prowadzonego procesu oraz poziomu jego powtarzalności wyniki mogą w pewnym stopniu różnić się od siebie o odchylenie standardowe. Po przekroczeniu założonego odchylenia wyrób uznaje się za niezdatny do użytku – mowa tutaj o tzw. skazach, niezgodności wymiarowej bądź gatunkowej. Im mniej odrzuconych elementów, tym lepiej, im bardziej powtarzalny proces, tym większa możliwość kontrolowania go. W fabrykach obserwujemy często duży przepływ personelu – ludzie przychodzą i odchodzą, pozostawiając po sobie metody, obliczenia, rozwiązania, czasami nawet całe zaprojektowane linie produkcyjne. Niestety, w zakładach, w których przykłada się mniejszą wagę do spełniania norm jakościowych – w odniesieniu do postępowania produkcyjnego, nie zaś jakości samych wyrobów finalnych – może dojść do sytuacji, w której występuje potrzeba zduplikowania linii produkcyjnej, jednak niestety nikt nie dysponuje odpowiednią dokumentacją.

Ponadto podczas pracy w produkcji wypracowuje się know-how, czyli zestaw rozwiązań i swoistych trików, które zapewniają powodzenie i większą efektywność procesu. Niestety, rzadko kiedy dokumentuje się know-how, część zmian w ustawieniach maszyn wprowadzana jest na bieżąco, co tym bardziej utrudnia ich powielanie. W takiej sytuacji z odsieczą przychodzi reverse engineering. Wewnętrzni specjaliści firmy bądź zewnętrzni eksperci ds. pomiarów 3D, wymiarowania i inżynierii odwrotnej są w stanie na podstawie istniejącego układu stworzyć taki sam bez aktualnych schematów czy informacji o parametrach procesu. Wykorzystuje się skanery 3D i tzw. trackery w celu ustalenia konkretnego położenia poszczególnych elementów układu względem siebie – dokładność do mikrometra zapewniana jest jedynie przez najlepszy sprzęt dostępny na rynku, konieczne więc będzie zaangażowanie firmy zewnętrznej, która już dysponuje tego typu sprzętem pomiarowym. Na podstawie wykonanych pomiarów można sporządzić wirtualną kopię linii produkcyjnej. Następnie każdy z jej elementów opisuje się, sczytując parametry maszyn z istniejącego układu w czasie pracy – temperatura procesu, czas wykonywania danej czynności, wymagany poziom czystości, wykorzystane narzędzia i nakładki oraz wszystkie inne niezbędne dane, które wymagają przeniesienia na układ numer dwa. Zaletą tworzenia cyfrowej kopii linii produkcyjnej czy układu maszyn jest to, że można z jej wykorzystaniem symulować pracę i oszacować wyniki w zależności od parametrów procesu. Po raz pierwszy mamy szansę zweryfikować bezstratnie, co się stanie, jeśli podwyższymy temperaturę, przyspieszymy daną czynność lub zmienimy skład chemiczny materiału wejściowego. Środowiska tego typu są trudne w obsłudze i programowaniu, dają jednak relatywnie wiarygodne dane wyjściowe, mogące następnie posłużyć do poprawy układu, nie tylko jego duplikacji.

Niestety, czasami inżynieria odwrotna wymaga ingerencji fizycznej w istniejący układ. Jeśli część sprzętu jest zabudowana, a nie posiadamy dokumentacji technicznej, specjaliści zmuszeni są rozłożyć układ na części. Element po elemencie opisuje się całość zespołu, w celu utworzenia odpowiedniej dokumentacji, która w przyszłości będzie mogła być wykorzystana do wielokrotnej duplikacji. To bardzo trudny i czasochłonny proces, który wiąże się z przestojem

produkcyjnym. Przed podjęciem takich prac konieczne jest skrupulatne zaplanowanie ewentualnych strat, czasu poszczególnych działań oraz przewidywanie problemów, które mogą wystąpić podczas działania. Cała operacja jest obarczona sporym ryzykiem, warto więc zaangażować zewnętrznego eksperta, który ma już doświadczenie w przeprowadzaniu podobnych działań.

## REVERSE ENGINEERING OPROGRAMOWANIA

Inżynierię odwrotną wykorzystuje się także do analizy działania oprogramowania. To szybko rozwijająca się odnoga inżynierii oprogramowania, służąca głównie do powielania już istniejących rozwiązań. Mowa tutaj zarówno o odtwarzaniu ścieżek pracy maszyn w oparciu o binarny kod wynikowy, jak i o powielaniu funkcjonalności oprogramowania w przypadku utraty kodu źródłowego [1, 2]. Działania tego typu podejmowane są zarówno przez firmy, które dane oprogramowanie rozwijają od lat, jednak nie posiadają już pełnej dokumentacji kodu źródłowego, jak i przez przedsiębiorstwa konkurencyjne, które na podstawie sposobu działania oprogramowania są w stanie określić, w jaki sposób zostało ono napisane. Jest to o tyle niebezpieczne, że działania tego typu są wykorzystywane przez tzw. crackerów do uzyskiwania dostępów do systemów informatycznych w celu np. jego uszkodzenia, wyciągnięcia pewnych danych, wprowadzenia zmian, przekazania dostępu osobom trzecim. Ta odsłona inżynierii odwrotnej może więc być postrzegana jako potencjalne zagrożenie dla firm operujących chronionymi danymi. Stąd ogromny nacisk na bezpieczeństwo informacji, który obecnie kładziony jest zarówno w przemyśle, jak i w IT. Istnieją podręczniki opisujące metody i narzędzia, które można wykorzystać w inżynierii odwrotnej [1]. Dział ten ma oczywiście dużo pozytywów, ponieważ czasami firmy korzystają z oprogramowania przez wiele lat, jego dostawca nie jest już na rynku, a konieczne jest wprowadzenie zmian i poprawek w kodzie. Wówczas zewnętrzna firma programistyczna może odtworzyć kod źródłowy i dostarczyć zmodyfikowane rozwiązanie, posiadające wszystkie stare funkcjonalności, a także wzbogacone o nowe.

## INŻYNIERIA ODWROTNA NA PRZYKŁADACH

Nietrudno o dobre przykłady wykorzystania inżynierii odwrotnej. Jednym z nich może być duplikowanie już istniejącego implantu. Jednym z urządzeń, które mogą zostać wykorzystane w tym procesie, jest skaner 3D. Implanty, np. płytki do stabilizacji odłamów kostnych, są zazwyczaj elementami niewielkich rozmiarów, przez co wystarczające mogą tutaj być skanery ręczne – szczytujące dane zarówno o geometrii wyrobu, jak i jego powierzchni. Obie te opcje są istotne w przypadku implantów, gdyż chropowatość i stan powierzchni są ważne podczas implantacji. Wymiary kopii muszą być takie same jak wymiary oryginału. Możliwe jest tutaj – jak zawsze w przypadku skanowania 3D – stworzenie wirtualnej kopii wyrobu, cyfrowego modelu, który można modyfikować przed wytworzeniem. W przypadku implantów niezwykle istotny jest sam proces produkcyjny, ponieważ muszą one posiadać nie tylko odpowiedni rdzeń materiałowy, lecz także określoną budowę warstwy powierzchniowej. To od niej zależy osiągnięcie niezbędnej biokompatybilności wyrobu. Należy zwrócić uwagę na własności mechaniczne, fizyko-chemiczne, magnetyczne oraz ewentualną odpowiedź biologiczną organizmu na ingerencję z zewnątrz. Każde środowisko ciała człowieka, np. środowisko układu kostnego, krwi, układu moczowego itd., wymaga odpowiedniego dostosowania implantu. Elementem

> ZALETĄ TWORZENIA CYFROWEJ KOPII LINII PRODUKCYJNEJ CZY UKŁADU MASZYN JEST TO, ŻE MOŻNA Z JEJ WYKORZYSTANIEM SYMULOWAĆ PRACĘ I OSZACOWAĆ WYNIKI W ZALEŻNOŚCI OD PARAMETRÓW PROCESU. MAMY SZANSĘ ZWERYFIKOWAĆ BEZSTRATNIE, CO SIĘ STANIE, JEŚLI PODWYŻSZYMY TEMPERATURĘ CZY PRZYSPIESZYMY DANĄ CZYNNOŚĆ.

inżynierii odwrotnej będzie więc tutaj odpowiedź na kilka ważnych pytań. W jakich warunkach oraz jak długo dany implant powinien pracować? Na jakie obciążenia i czynniki propagujące procesy korozyjne będzie narażony? Czy podczas pracy musi zmieniać swój kształt, czy też pozostaje w niezmienionej formie? Czy powinien uwalniać leki do okolicznych tkanek, a jeśli tak – w jakim czasie oraz w jaki sposób? Finalnie, jeśli gotowy implant spełnia określone pierwotnie warunki, to jak został wytworzony oraz w jakiej kolejności przeprowadzano etapy produkcyjne? Jak widać, w tym przypadku mamy do czynienia ze złożonym procesem, w którym nie ma miejsca na błędy, mogą się one bowiem zakończyć uszczerbkiem na zdrowiu pacjenta.

Inżynierię odwrotną można jednak spotkać także w mniej produkcyjnych warunkach. Dobrym przykładem na jej użycie jest bowiem odzwierciedlenie miejsc zbrodni z wykorzystaniem skanerów 3D i trackerów. Dzięki wykonaniu precyzyjnych pomiarów odległości poszczególnych obiektów w obszarze miejsca zbrodni możliwe jest dokładne odzwierciedlenie wydarzeń, krok po kroku, co znacznie ułatwia rozwiązanie sprawy kryminalnej. Skanery 3D służą tutaj do stworzenia wirtualnego obrazu miejsca zbrodni, który następnie wykorzystywany jest do przeprowadzania symulacji kolejności zdarzeń w feralnym dniu. Ofiara prowadzi nas do zabójcy – w tym przypadku jej ułożenie ciała, przedmiotów w pomieszczeniu, ślady po kulach, położenie pocisków i łusek, ewentualna broń w miejscu zbrodni, ślady krwi, przewrócone meble czy otwarte okno. Liczy się każdy element, a tworzone krok po kroku wirtualne środowisko skrupulatnie opowiada historię morderstwa. Inżynieria odwrotna jest więc obecna nie tylko w życiu pracowników produkcji czy inżynierów na co dzień pracujących z zaawansowanymi technologiami, lecz wpływa na codzienne losy nas wszystkich, asystując w rozwiązywaniu skomplikowanych problemów i wyzwań. ■

### Źródła


1. Yurichev D., *Reverse engineering for beginners*, https://beginners.re/RE4B-EN.pdf [dostęp: 10.09.2017].
2. Reverse Engineering, SearchSoftwareQuality, http://searchsoftwarequality.techtarget.com/definition/reverse-engineering [dostęp: 10.09.2017].