1.1 Assurance case – definicja i struktura

Koncepcja Assurance Case znajduje zastosowanie w dziedzinie wytwarzania oprogramowania, dla którego istnieją zdefiniowane wymagania w zakresie cech takich jak: bezpieczeństwo, niezawodność, łatwość obsługi oraz utrzymywania.

Często, w nawiązaniu do tej koncepcji spotyka się definicję, iż jest to uzasadniony, nieodparty argument wspierany przez materiał dowodowy, którym system, usługa lub organizacja będą zarządzać w przeznaczonym do tego zdefiniowanym środowisku lub aplikacji.

Model Assurance Case sprawdza się podczas przeprowadzenia kompletnego wnioskowania o prawdziwości roszczenia (clime) , które z reguły przyjmuje postać rzeczywistej cechy systemu. Udowodnianie prawdziwości roszczenia na drodze wnioskowania odbywa się tak samo, niezależnie od tego czy będziemy dowodzić o bezpieczeństwie systemu czy np. jego niezawodności. Przyjęto konwencję nazywania modelu Assurance Case od nazwy cechy, której prawdziwość ma zostać wykazana. Wyróżnia się zatem: Safety Cases w których zadaniem jest potwierdzenie prawdziwości twierdzenia że system jest bezpieczny w określonym kontekście użycia[[1]](#footnote-1). Norma IEEE ISO 15026-2 oprócz podanego wyżej Safety Case, wyróżnia także inne „formy” modelu Assurance Case tj. Reliabilty Case – w przypadku kiedy zamierzamy wnioskować na temat niezawodności systemu, oraz Maintainability Case – jeśli przedmiotem przeprowadzenia wnioskowania jest cecha polegająca na łatwości utrzymania systemu lub określnie poziomu trudności jego obsługi[[2]](#footnote-2).

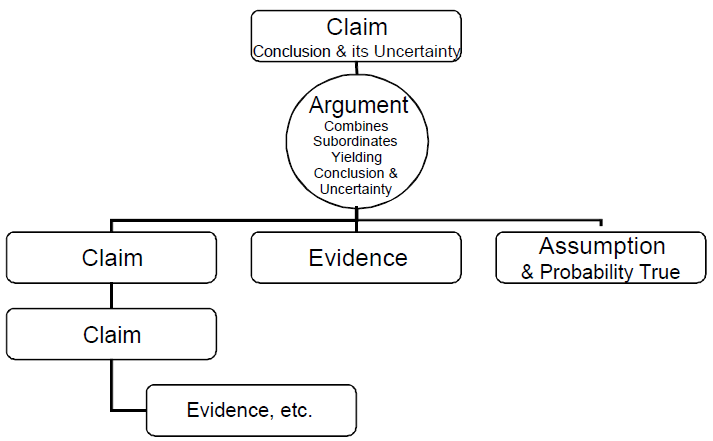
Zasadą tworzenia modelu Assurance Case jest podział celu nadrzędnego (np.: wykazanie dowolnej cechy systemu lub produktu) na mniejsze twierdzenia których prawdziwość łatwiej jest jednoznacznie wykazać. Takie działanie prowadzi do powstania pewnej hierarchii twierdzeń których zgodność o ile to możliwe będzie jednoznacznie określona i potwierdzona. Zachowanie prawidłowej struktury w Assurance Case jest o tyle ważne, że ułatwia łatwy i logiczny przegląd procesu wnioskowania.

Pewność z jaką możemy wykazywać cechy systemu używając modelu Assurance Case powoduje że odgrywa on istotną rolę np. w kontekście wewnętrznego badania jakości wytworzonego przez firmę oprogramowania przed dystrybucją na rynek.

Istotną korzyścią, która rekompensuje nakład czasu i pracy przy tworzeniu Assurance Case jest łatwiejsze uzyskanie pozytywnego wyniku w procesie certyfikacji oprogramowania przez instytucję zewnętrzną. Niektóre instytucje przeprowadzające certyfikacje oprogramowania zwłaszcza w zakresie bezpieczeństwa mogą wprost wymagać przedstawienia przez dostawcę dowodu na określony poziom bezpieczeństwa systemu.

Innym korzystnym zjawiskiem jakie wytwarza stosowanie modelu Assurance Case jest jego efekt marketingowy. Zapewnienie potencjalnego klienta o bezpieczeństwie systemu, niezawodności czy łatwości utrzymania / obsługi staje się łatwiejsze jeśli jest uargumentowane na wytworzonym w tym celu czytelnym modelu[[3]](#footnote-3).

Wnioskowanie za pomocą Assurance Case jest możliwe dzięki jego konstrukcji spójnych ze sobą elementów tj. roszczeń (climes), argumentów (arguments), dowodów (evidences) oraz twierdzeń (assumptions).



Niniejsza praca dyplomowa, skupiać się będzie na systemach stosowanych w urządzeniach medycznych. Oczywistym wymaganiem tych systemów jest pewność co do ich bezpieczeństwa stąd w tej pracy już na etapie przedstawiania podstawowych ogólnych informacji odwoływał się będę do modelu Safety Case.

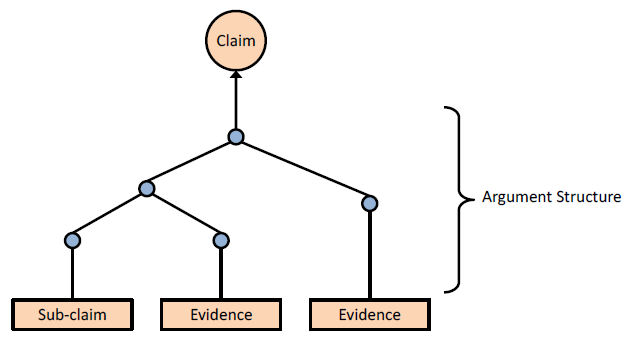
Koncepcja Safety Case narodziła się na terenie Wielkiej Brytanii skąd w latach sześćdziesiątych XX w. rozprzestrzeniała się na inne kraje europejskie oraz Australię. Podejście wg tej koncepcji do wnioskowania o akceptowalnym poziomie bezpieczeństwa było szeroko wykorzystywane w szczególnie krytycznych gałęziach przemysłu których częścią są elektrownie atomowe, zakłady przemysłowe, transport a także zamówienia w dziedzinie obronności.

Początek XX wieku wytworzył kolejny obszar zastosowania dla koncepcji Safety Case. Mam tu na myśli programy kosmiczne, gdzie wysoki priorytet niezawodności systemów wymusza badanie i rozwój metodologii wnioskowania o bezpieczeństwie. inżynierowie NASA (National Aeronautics and Space Administration) porównują koncepcję Safety Case do procesu decyzyjnego w którym wykazanie bezpieczeństwa opiera się na identyfikacji i szacowaniu ryzyk systemu oraz poszukiwaniu równowagi między bezpieczeństwem a jego wydajnością w pozostałych obszarach (koncepcja RISC: risc-informed safety case). Zastosowanie tej koncepcji daje wyraźny sygnał że organizacja wytwarzająca system / oprogramowanie bierze pełną odpowiedzialność za zapewnienie że jest on akceptowalnie bezpieczny. Osoby decyzyjne w procesie wnioskowania o bezpieczeństwie w trakcie całości procesu mają pełną kontrolę nad tym, że w każdym „kluczowym punkcie decyzyjnym” cele w zakresie bezpieczeństwa systemu zostały osiągnięte. Ważność, aktualność procesu decyzyjnego w koncepcji RISC jest uzależniona od zastosowania budowanego systemu w określonym środowisku. Konieczne jest zatem aby stosując tą koncepcję określić środowisko / otoczenie operacyjne systemu w którym jest on uważany za bezpieczny. Jeśli w trakcie przeszukiwania środowiska zostaną znalezione nieaktualne zastrzeżenia o bezpieczeństwie można wnioskować że system nie spełnia już wymogów bezpieczeństwa. Główne elementy w strukturze RISC to:

* Zestaw roszczeń lub roszczenie, spójnych pod względem zapewnienia że nadrzędne cele operacyjne określone dla bezpieczeństwa systemu zostały spełnione. Inaczej mówiąc jest to główne roszczenie (clime), że system jest odpowiednio bezpieczny.
* Dowody (evidence) stosowane jako podstawa dla argumentu o bezpieczeństwie. Przeważnie są to fakty w postaci ustalonych zasad naukowych lub dane empiryczne.
* Ustrukturyzowane argumenty o bezpieczeństwie, połączone z dowodami, używające logicznie poprawnych reguł wnioskowania. Argumenty o bezpieczeństwie mogą być deterministyczne, probabilistyczne lub jakościowe[[4]](#footnote-4).

Dowody połączone z argumentami tworzą spójną strukturę (argument structure) obrazowaną przez digram w którym proces wnioskowania rozpoczyna się od elementów położonych najniżej.

Opisaną strukturę koncepcji RiSC przedstawia poniższy schemat:



Rysunek 1. Schemat wnioskowania o bezpieczeństwie systemu wg. koncepcji RISC[[5]](#footnote-5).

Przedstawiona wyżej koncepcja RiSC to oczywiście nie jedyne podejście do Safety Case kreowane w sferze inżynierii oprogramowania.

Europejska organizacja ds. bezpieczeństwa żeglugi powietrznej (Eurocontrol) w dokumencie „Safety Case Development manual” wskazuje, że większość jeśli nie wszystkie modele Safety Case można podzielić na dwie kategorie: Unit Safety Cases – stosowane w celu wykazania bezpieczeństwa w sposób ciągły, oraz Project Safety Cases – wykorzystywane do prezentowania jedynie istotnych zmian mających wpływ na poziom bezpieczeństwa. Unit Safety Cases są produkowane i utrzymywane w celu wykazania że bieżące wykonywane z dnia na dzień operacje są bezpieczne z punktu widzenia całego systemu. Informacje w nim przechowywane zawierają określenie szacowanego poziomu bezpieczeństwa systemu / usługi (w danym czasie) oparte na zapisie monitoringu operacyjnego, ankiet czy rezultatów audytu bezpieczeństwa. Taki zbiór informacji ma na celu dokładane określenie ostatniego momentu w czasie w którym stwierdzono że system / usługa jest akceptowalnie bezpieczna w zakładanym kontekście użycia.

Project Safety Case ma na celu prezentację jedynie tych zmian które miały istotny wpływ na poziom bezpieczeństwa systemu lub obsługi. Ryzyka uwzględniane przez tą kategorię Safety Case są tworzone lub modyfikowane w wyniku zmian wprowadzanych do systemu lub usługi. Opierają się one na założeniach lub dowodach z powiązanego modelu Unit Safety Case, że konfiguracja usługi lub systemu przed wprowadzeniem zmian realizowała podstawowe cele w zakresie bezpieczeństwa[[6]](#footnote-6).

Niezależnie od wybranego rodzaju Safety Caase elementarną jego częścią jest roszczenie o bezpieczeństwie (safety case clime) które należy udowodnić w procesie wnioskowania. Wspomniana wyżej koncepcja RiSC opracowana przez inżynierów NASA zakłada istnienie dwóch niezależnych typów roszczeń o bezpieczeństwie systemu:

* Roszczenia powiązane z bieżącą lub wcześniejszą fazą wnioskowania w której podstawowe kryteria w zakresie zapewnienia bezpieczeństwa zostały spełnione
* NASA safery handbook

1. Origin Consulting (York) Limited, on behalf of the Contributors, " GSN community standard version 1", November 2011, s. 9 [↑](#footnote-ref-1)
2. IEEE ISO 15026-2 System Assurance - Assurance Case, s. 20-21 [↑](#footnote-ref-2)
3. Beata Maria Łuczak, "Ocena narzędzi do budowy Assurance Case", PG 2014, s. 8 [↑](#footnote-ref-3)
4. H.Dezfuli, A.Benjamin, Ch. Everett, C.Smith, M.Stamatelatos, R. Youngblood, "NASA system safety handbook", NASA Nov 2011 , s. 69 - 71 [↑](#footnote-ref-4)
5. H.Dezfuli, A.Benjamin, Ch. Everett, C.Smith, M.Stamatelatos, R. Youngblood, "NASA system safety handbook", NASA Nov 2011 , s. 72 [↑](#footnote-ref-5)
6. „Safety Case Developement manual” s. 6 - 7 [↑](#footnote-ref-6)