## *Assurance Case – definicja i struktura*

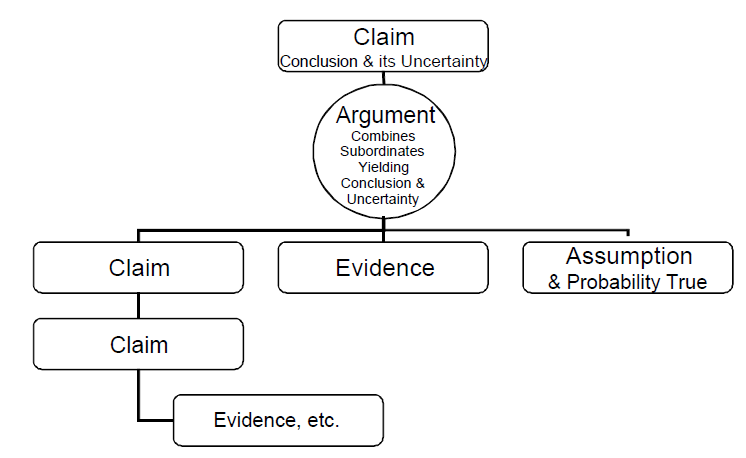
Fundamentem pozwalającym zapoznać się z tematyką argumentacji wiarygodności systemów jest wiedza o Assurance Case. Pojęcie to łączy w sobie m.in.: twierdzenie lub zestaw twierdzeń wysokiego poziomu traktujących o własnościach systemu lub produktu, usystematyzowaną argumentację na poparcie wspomnianych twierdzeń oraz dowody i jednoznaczne założenia, które podlegają tym argumentom[[1]](#footnote-1). Geneza tego wyrażenia jest związana pojęciem safety case. Definicja tego wyrażenia zamyka się do uzasadnienia bezpieczeństwa systemu i przedstawienia czynności zmierzających do jego osiągnięcia. Określenie Assurance Case operuje na wyższym stopniu ogólności ponieważ nie odnosi się tylko do udowodnienia określonego poziomu bezpieczeństwa systemu ale pozwala także wykazać inne jego cechy np.: zgodność z istniejącymi normami, awaryjność, łatwość w utrzymaniu, czy też stopień adaptacji do nowego otoczenia[[2]](#footnote-2). Zależnie od tego, jaką cechę systemu zamierzamy udowodnić wyróżnia się: reliabilty case – w przypadku kiedy zamierzamy określić niezawodność systemu, maintainability case – jeśli przedmiotem przeprowadzenia dowodu jest cecha polegająca na łatwości utrzymania systemu lub poziom trudności jego obsługi. Najbardziej popularnym zastosowaniem tego rodzaj wnioskowania są safety cases w których dowód przeprowadzany jest dla określenia poziomu bezpieczeństwa sytemu[[3]](#footnote-3).

Assurance Case ostatecznie prezentuje argument dla którego system jest akceptowalnie bezpieczny, niezawodny czy prosty w obsłudze. Należy jednak pamiętać, że określenie system może być rozumiane w kontekście oprogramowania sterującego, kombinacji oprogramowania i sprzętu czy np. systemu procedur wykorzystywanych w konkretnych sytuacjach (operating rules). Zapewnienie trwałej cechy danego systemu wymaga systematycznej aktualizacji struktury przeprowadzonego dowodu który ją udowadnia. Takie podejście jest ważne istotne szczególnie w kontekście systemów gdzie wymagany jest najwyższy poziom niezawodności[[4]](#footnote-4).

Model Assurance Case opiera się na „podziale” twierdzenia nadrzędnego, czyli cechy którą produktu którą zamierzamy udowodnić, na twierdzenia podrzędne o mniejszym zakresie ale łatwiejsze do wykazania ich prawdziwości. Prawidłowo zbudowana struktura assurance case „od ogółu do szczegółu” powiązana z materiałem dowodowym powinna pozwalać na jasne wnioskowanie o całości twierdzenia. Każdy podrzędny element struktury odpowiednio potwierdzony w materiale dowodowym, którego prawdziwość wywnioskowano jest istotny w kontekście określenia czy sformułowany wniosek np.: czy system jest bezpieczny jest prawdziwy.

Wnioskowanie assurance case pod określonymi warunkami (np. aktualność składowych modelu) pozwala trafnie określić prawdziwość cechy systemu. Skuteczność takiego dowodzenia wykorzystano w aspekcie uregulowań prawnych dla systemów pracujących w środowiskach kluczowych dla gospodarki. Szczególne znaczenie ma tu zastosowanie safety case których wymagalność jest prawnie określona w krajach anglosaskich dla takich obszarów jak przetwórstwo paliw, energetyka, transport, służba zdrowia[[5]](#footnote-5).

Jednym z elementów modelu Assurance Case jest tzw. (High level argument) który wyjaśnia w jaki sposób dostępne dowody powinny być interpretowane w kwestii określenia akceptowalnego działania systemu. Taką interpretację materiału dowodowego uzyskuje się przez wykazanie ich zgodności z wymaganiami stawianymi systemowi. Ważną rolę modelu udowadniania wiarygodności systemu pełnią dowody (evidence). Najprościej mówiąc są to po prostu wyniki obserwacji, testów uzyskanych za pomocą badań, symulacji które dostarczają informacji na temat określonych właściwości systemu. Dowody są powiązane z wnioskiem podlegającym udowodnieniu za pomocą argumentów[[6]](#footnote-6).



Rys.1 Fragment Struktury Assurance Case Źródło: Źródło: IEEE ISO 15026-1 System Assurance - Vocabulary, s. 11

Znacznie dokładniejsze informacje na temat struktury Assurance Case można odnaleźć w normie ISO: 15026-2. Dokument ten wylicza własność modelu Assurance Case takie jak:

1. Posiadanie jednego lub kilku twierdzeń wysokiego poziomu które mają zostać udowodnione przez „spięte” z nimi argumenty. Jeśli istnieje więcej niż jedno twierdzenie którego prawdziwość należy wykazać wówczas dla spójności wnioskowania rozpatruje się ich koniunkcję,
2. Argument powinien być wspierany przez jedno lub więcej twierdzeń, dowodów lub założeń. Rolą argumentu w modelu Assurance Case jest pokazanie zależności pomiędzy dowodem a twierdzeniem lub twierdzeniami które należy udowodnić. Argument powinien posiadać komponent (czyli zestaw dowodów lub twierdzeń niskiego poziomu) który jest z nim związany w trakcie procesu wnioskowania.

Jeśli jeden argument nie może bezpośrednio wspierać innego argumentu to argument niższego poziomu powinien zostać dołączony do twierdzenia niższego poziomu które z kolei jest powiązane z argumentem wyższego poziomu.

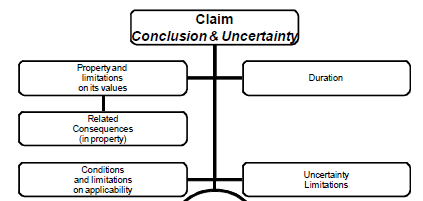
1. Twierdzenie powinno być wspierane przez jeden argument lub jedno bądź więcej, twierdzeń, dowodów, założeń. Jeden i tylko jeden argument może wspierać wniosek wysokiego poziomu. Alternatywnie jedno twierdzenie może być wspierane ( bezpośrednio, nie przez argument) przez klika zestawów dowodów, założeń lub twierdzeń niskiego poziomu.
2. Wnioski, argumenty, dowody, założenia nie wspierają się pośrednio lub bezpośrednio lecz użyte pojedynczo stanowią wsparcie dla wieloskładnikowych komponentów[[7]](#footnote-7).

Rozważmy bardziej szczegółowo każdy element modelu Assurance Case. Norma ISO: 15026-2 określa że wniosek to prawdziwe lub fałszywe stwierdzenie które jednoznacznie określa właściwości wniosku, ograniczenia w zakresie ufności w stosunku do tych właściwości a także ograniczenia dla których uznaje się wniosek za zasadny.

Poprawnie sformułowany wniosek składa się z trzech typów elementów: wymaganych, warunkowo wymaganych, opcjonalnych. Składowe wymagane to m.in. właściwości wniosku, rangi „ważności” własności powiązanych z wnioskiem, wartości graniczne w których wyraża się stopień pewności co do własności wniosku, ograniczenia w zakresie warunków dla jakich wniosek jest uznany za trafny. Opcjonalne elementy wniosku to: ograniczenia w zakresie czasu w którym wniosek może zostać uznany za trafny, ograniczenia w zakresie czasu w którym możemy powiedzieć że wniosek jest jednoznacznie fałszywy lub prawdziwy, warunki pewności względem wniosku. Ostatnią kategorią elementów wniosku są te które uznaje się za wymagane ale tylko w określonych warunkach m.in.: konsekwencje lub ryzyka jakie związane z formułowanym wnioskiem a także wskazanie czy występowanie konkretnej właściwości wniosku dotyczy np. określonej wersji, podzbioru systemów lub produktów.

Elementy wymagane oraz opcjonalne często operują w zakresie określenia „ograniczenia”. Dokument ISO wspomniany wyżej traktuje szerzej jak należy rozumieć takie określenie. Termin ograniczenia jest używany w celu dopasowania do wielu sytuacji które mogą występować. Wartości ograniczeń poszczególnych elementów mogą występować jako pojedyncze wartości, lub zbiór pojedynczych wartości, pojedyncza ranga lub zbiór rang, Uwzględnia się także przypadki wielowymiarowości wartości ograniczeń poszczególnych elementów. Zakresy ograniczeń elementów składowych wniosku w modelu Assurance Case często obejmują rozkład prawdopodobieństwa, mają charakter przyrostowy lub przyjmują postać innych aspektów rozmytych.

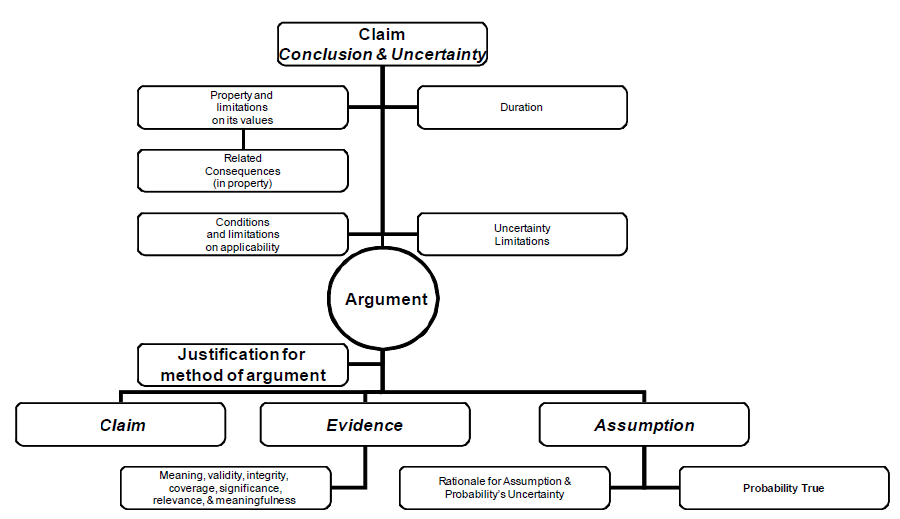
Wybór wniosku najwyższego poziomu i określenie jego właściwości jest krytyczne względem dalszego konstruowania modelu Assurance Case. Istotne zatem jest dołączenie uzasadnienia na którym opieramy decyzję o umieszczeniu tego wniosku na szczycie drzewa w konstrukcji modelu. Publikowanie uzasadnień ułatwia poprawne zrozumienie modelu wszystkim którzy są zainteresowani jego analizą[[8]](#footnote-8).



Rys.2 Budowa wniosku w strukturze Assurance Case Źródło: IEEE ISO 15026-1 System Assurance - Vocabulary, s. 23

Dokładne zrozumienie roli wniosku w Assurance Case jest istotne w kontekście opisania kolejnego elementu modelu jakim jest argument. Norma IEEE ISO 15026-2 charakteryzuje argument podając powody dla których jest on używany w modelu Assurance Case. Element ten jest potrzebny do pokazania w jaki sposób komponenty leżące bezpośrednio u jego podstawy odnoszą się do zastrzeżenia lub zbioru zastrzeżeń. Rola argumentu wzrasta jeśli występuje on w formie kalkulacji inżynieryjnej lub dowodu logicznego. Istotnymi cechami każdego argumentu są m.in. konieczność posiadania wniosków dotyczący każdego wspieranego zastrzeżenia. Argument powinien ustalać zakres niepewności każdego ustalonego przez siebie wniosku. Wymagane jest aby argument posiadał informacje na temat tego w jaki sposób może wpływać na niepewność podległych wniosków. Przedstawienie argumentu powinno być spójne względem komponentów położonych bezpośrednio pod nim. Ważną informacja na temat argumentu w modelu Assurance Case jest to, że powinien on posiadać skojarzone uzasadnienie dla ważności lub wartości jego „metody rozumowania” np. obliczanie lub tok argumentowania. Metody rozumowania stosowane w zakresie konstrukcji argumentu są zróżnicowane. Narzędzia używane przez te metody mają różną stosowalność, moc, dokładność i niepewność oraz łatwość użycia.

Specyfika konstrukcji Modelu Assurance Case zakłada używanie argumentów do poparcia lub osłabienia zastrzeżeń. Argumenty mają wpływ na niepewność skojarzonych z nim zastrzeżeń.



1. IEEE ISO 15026-2 System Assurance - Assurance Case, s. 20 [↑](#footnote-ref-1)
2. Beata Maria Łuczak, "Ocena narzędzi do budowy Assurance case", praca mgr, PG 2014, s. 8 [↑](#footnote-ref-2)
3. IEEE ISO 15026-2 System Assurance - Assurance Case, s. 20-21 [↑](#footnote-ref-3)
4. Charles B. Weinstock, "Assurance cases" , Carnegie Mellon University, Pittsburg 2008, str. 27 [↑](#footnote-ref-4)
5. Beata Maria Łuczak, "Ocena narzędzi do budowy Assurance Case", praca mgr, PG 2014, s. 8 [↑](#footnote-ref-5)
6. Charles B. Weinstock, "Assurance cases" , Carnegie Mellon University, Pittsburg 2008, s. 29 [↑](#footnote-ref-6)
7. IEEE ISO 15026-2 System Assurance - Assurance Case, s. 20 [↑](#footnote-ref-7)
8. IEEE ISO 15026-2 System Assurance - Assurance Case, s. 21 [↑](#footnote-ref-8)