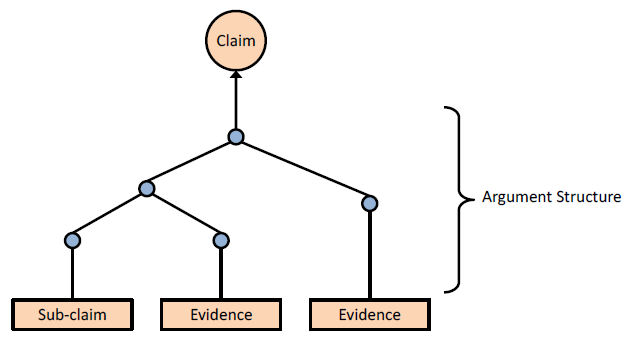
Metodologia dotycząca wnioskowania o bezpieczeństwie – Safety Case narodziła się na terenie Wielkiej Brytanii, skąd w latach sześćdziesiątych XX w. rozprzestrzeniała się na inne kraje europejskie oraz Australię. Dowodzenie o akceptowalnym w kontekście użycia, poziomie bezpieczeństwa jest szczególnie istotne w przypadku strategicznie ważnych gałęzi przemysłu. Trudno wyobrazić sobie brak realnego dowodu bezpieczeństwa systemów komputerowych stosowanych w energetyce, dużych zakładach przemysłowych, transporcie, przemyśle zbrojeniowym, medycynie i wielu innych obszarach aktywności gospodarczej ważnych dla ludzi. Konieczność potwierdzania bezpieczeństwa systemów jest ważna także z punktu widzenia projektów związanych z eksploracją kosmosu. Wytworzenie spójnego modelu, który umożliwiałby przeprowadzenie wnioskowania o bezpieczeństwie opartego na zebranych dowodach jest niezbędne w przypadku systemów sterowania, podtrzymywania życia w wahadłowcach, które umożliwiają wykonywanie załogowych lotów w kosmos. Wysokie priorytety w zakresie bezpieczeństwa w przypadku awarii, oraz niezawodności tych systemów stanowią przyczyny dla których istotne jest przeprowadzenie dowodu bezpieczeństwa w oparciu o aktualny i reużywalny model logiczny.

Inżynierowie NASA (National Aeronautics and Space Administration) utożsamiają dowód bezpieczeństwa - Safety Case z procesem decyzyjnym w którym wykazanie roszczenia o bezpieczeństwa opiera się na identyfikacji i szacowaniu ryzyk systemu. Kluczowe według nich jest znalezienie odpowiedniego poziomu równowagi pomiędzy bezpieczeństwem systemu a jego wydajnością. Tak sformułowane wnioski na temat dowodu bezpieczeństwa zostały ujęte w zakresie koncepcji RISC: (Risc-Informed Safety Case). Zastosowanie tej metodologii ma wysyłać do klientów wyraźny sygnał, że organizacja wytwarzająca system / oprogramowanie, bierze pełną odpowiedzialność za zapewnienie akceptowalnego poziomu bezpieczeństwa. Osoby decyzyjne w procesie wnioskowania o bezpieczeństwie systemu mają pełną wiedzę na temat tego czy postawione cele w zakresie bezpieczeństwa zostały osiągnięte w każdym „kluczowym punkcie decyzyjnym”. Ważność, aktualność modelu 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.

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[[1]](#endnote-1).

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[[2]](#endnote-2).

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

1. H.Dezfuli, A.Benjamin, Ch. Everett, C.Smith, M.Stamatelatos, R. Youngblood, "NASA system safety handbook", NASA Nov 2011 , s. 69 - 72 [↑](#endnote-ref-1)
2. „Safety Case Developement manual” s. 6 - 7 [↑](#endnote-ref-2)