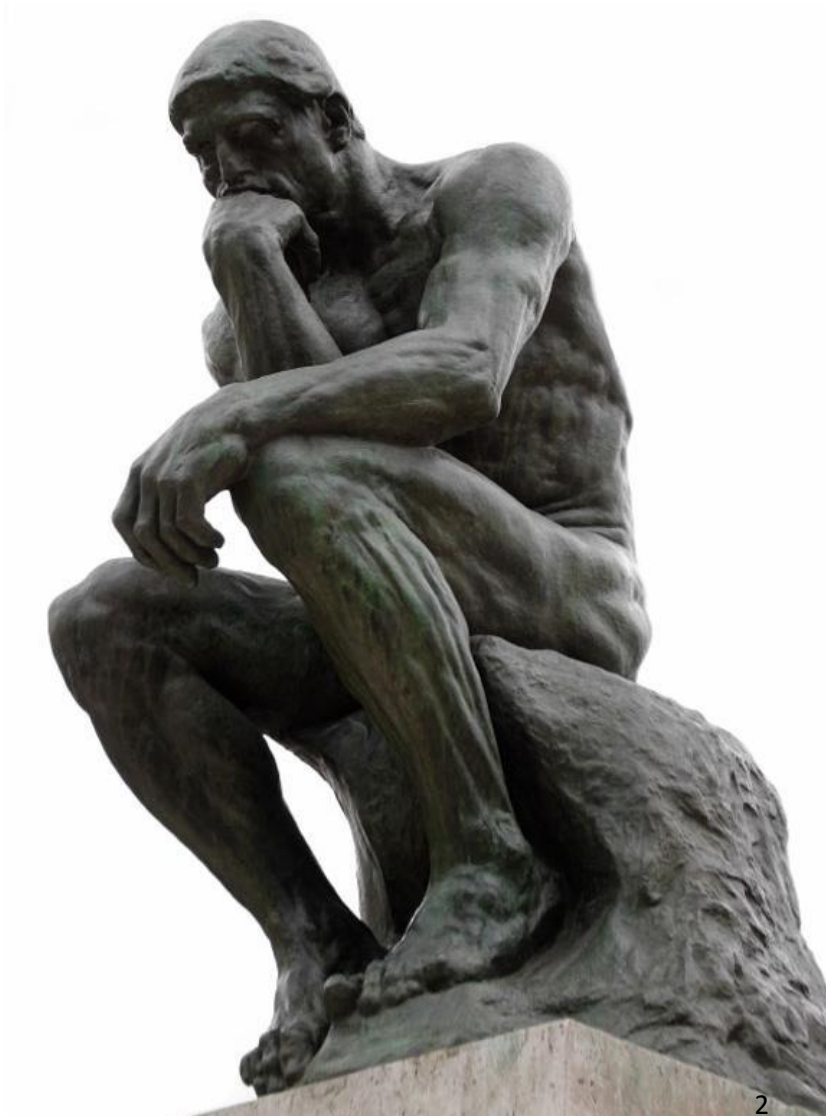
Analiza zakresu zmian argumentacji wiarygodności (*assurance case*) z użyciem metamodelu *evidence framework*

Andrzej Wardziński
Katedra Inżynierii Oprogramowania
Gdańsk, 14.04.2015

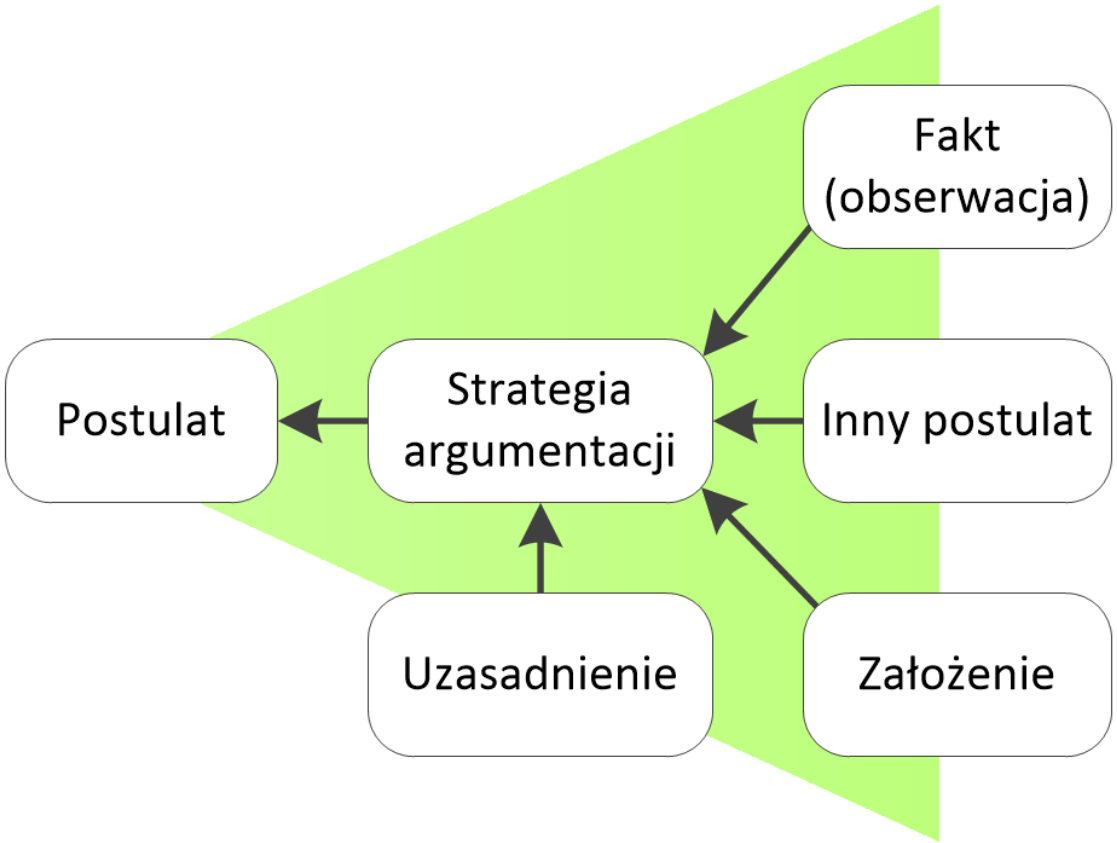
O czym dziś mowa?

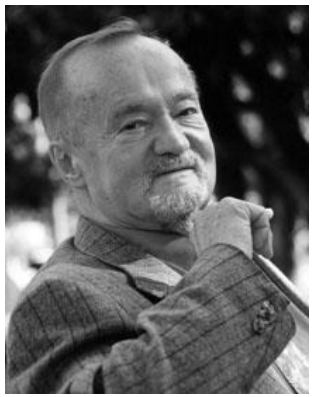
- Co to argumentacja wiarygodności (*assurance case*)?
- Argumentacja w cyklu życia systemu
- Zmiany argumentacji
- Perspektywy jako ścieżki propagacji zmian
- Metamodel *evidence framework*
- Przykład zmiany
- Podsumowanie

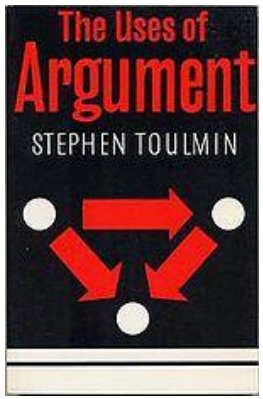


Struktura argumentacji

Argumentacja pokazuje w jednoznaczny, przekonujący i zrozumiały sposób wnioskowanie popierające postulat lub tezę.







Stephen Toulmin, 1922-2008
Twórca teorii argumentacji
„The Uses of Argument”, 1958

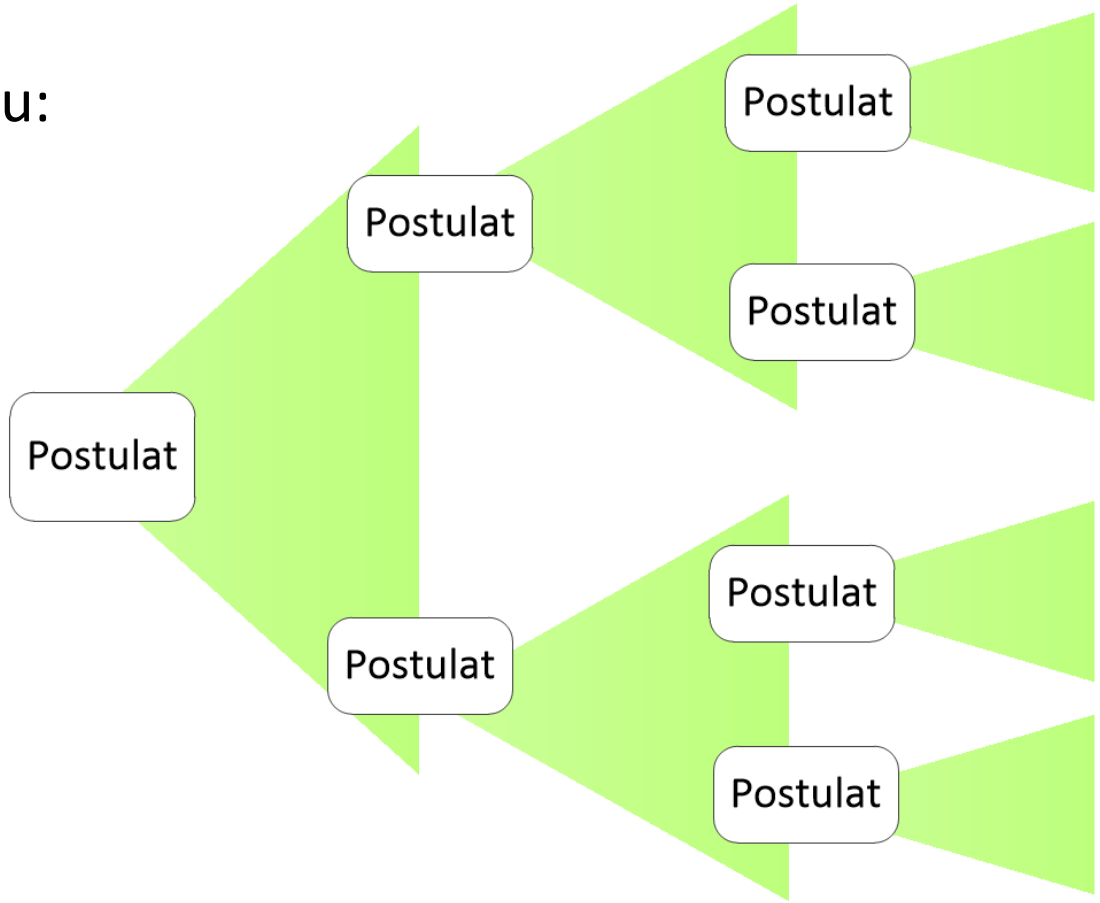
Poziomy argumentacji

Argumentację budujemy poziomami od głównego celu aż do szczegółowych przesłanek.

Każdy krok argumentacji jest jawnie określony.

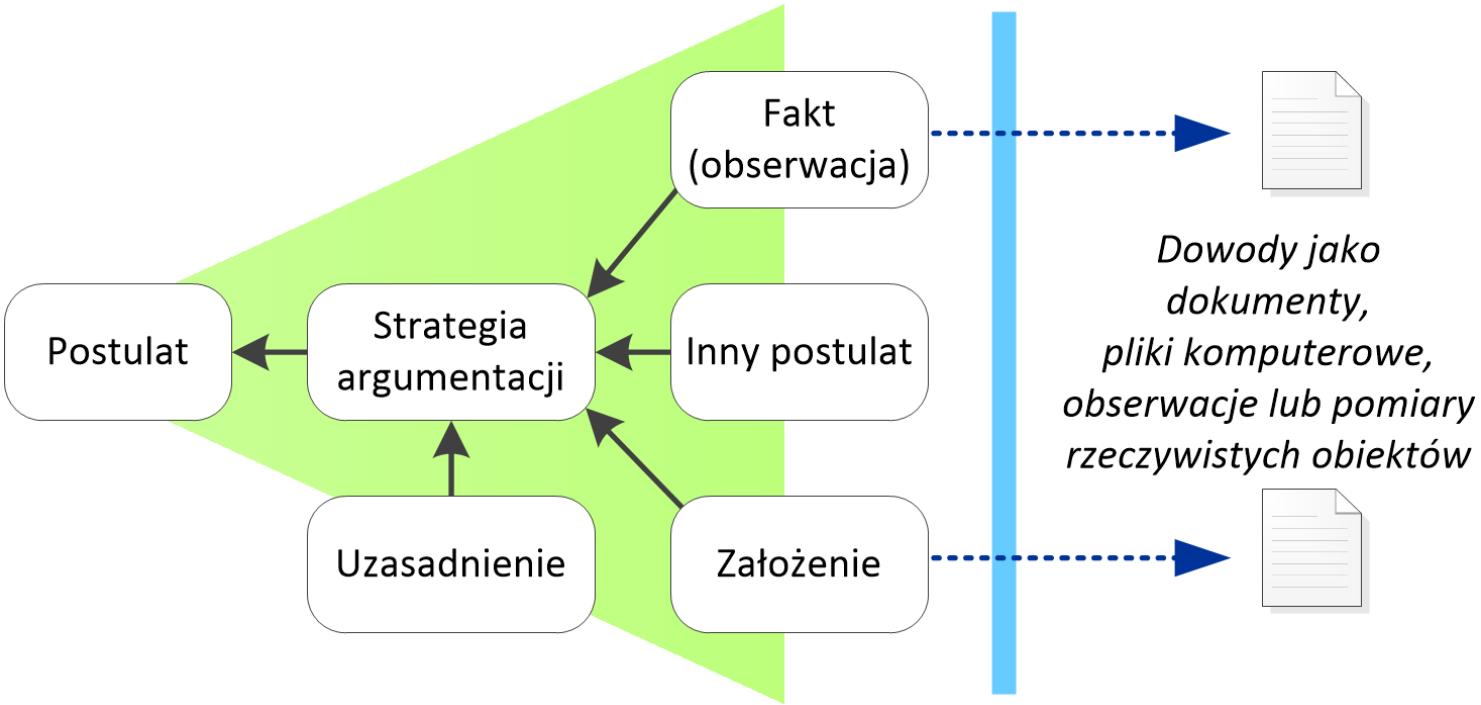
Przykłady głównego postulatu:

- System jest bezpieczny
- System spełnia wymagania…
- Organizacja spełnia wymagania…



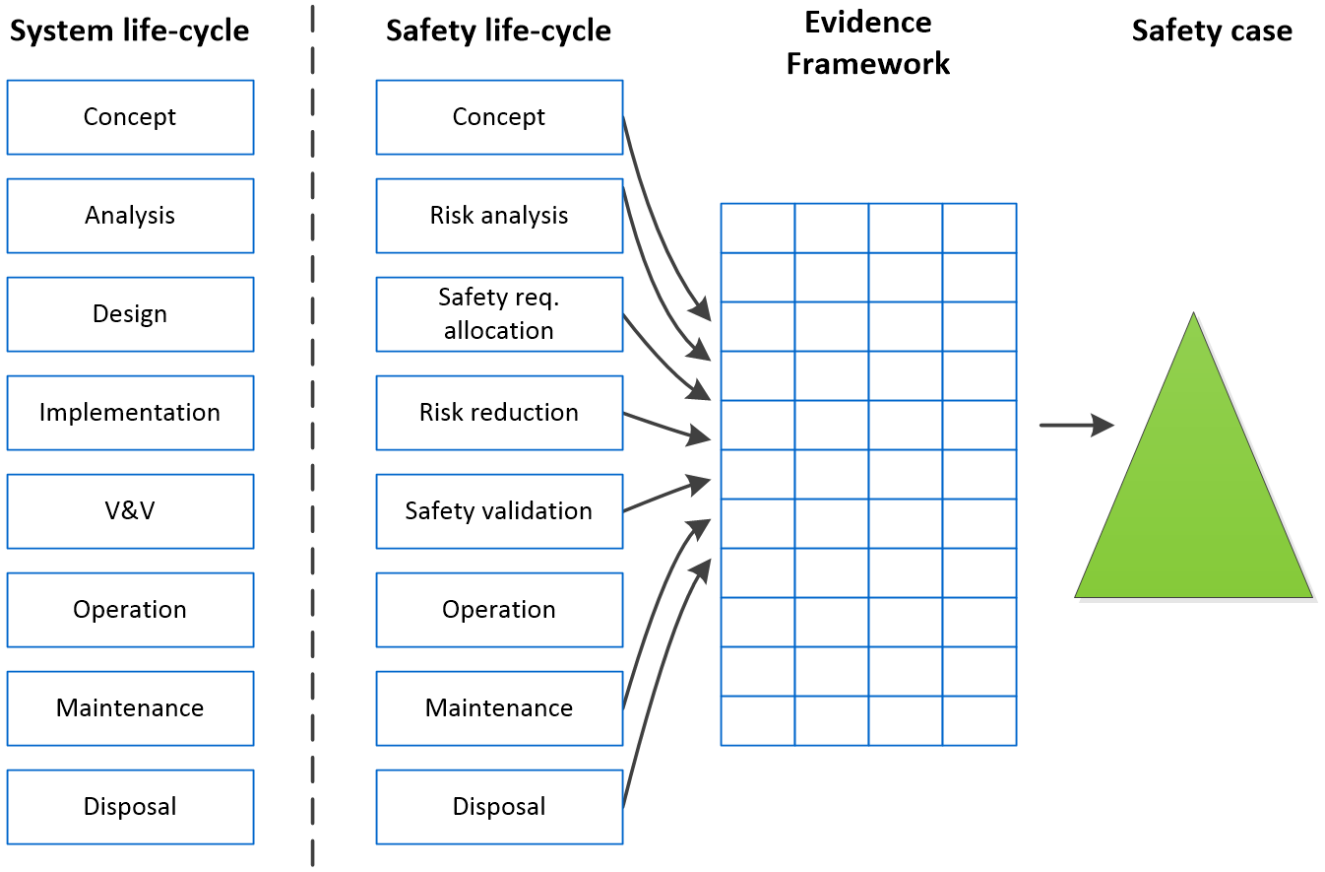
Argumentacja a obserwowany świat

- Końcowe elementy argumentacji odwołują się do świata rzeczywistego
- Mówimy, że dostarczamy **dowody** dla argumentacji
- Czy są dowody?
  - Czy jest to nieuporządkowany zbiór dokumentów?
  - Czy jest to jakaś spójna całość?



Argumentacja w cyklu życia systemu

Evidence framework = spójny zbiór dowodów



evidence framework
structure identifying what evidence will be/has been produced and when

IEC 62741/Ed1: Demonstration of dependability requirements – The dependability case

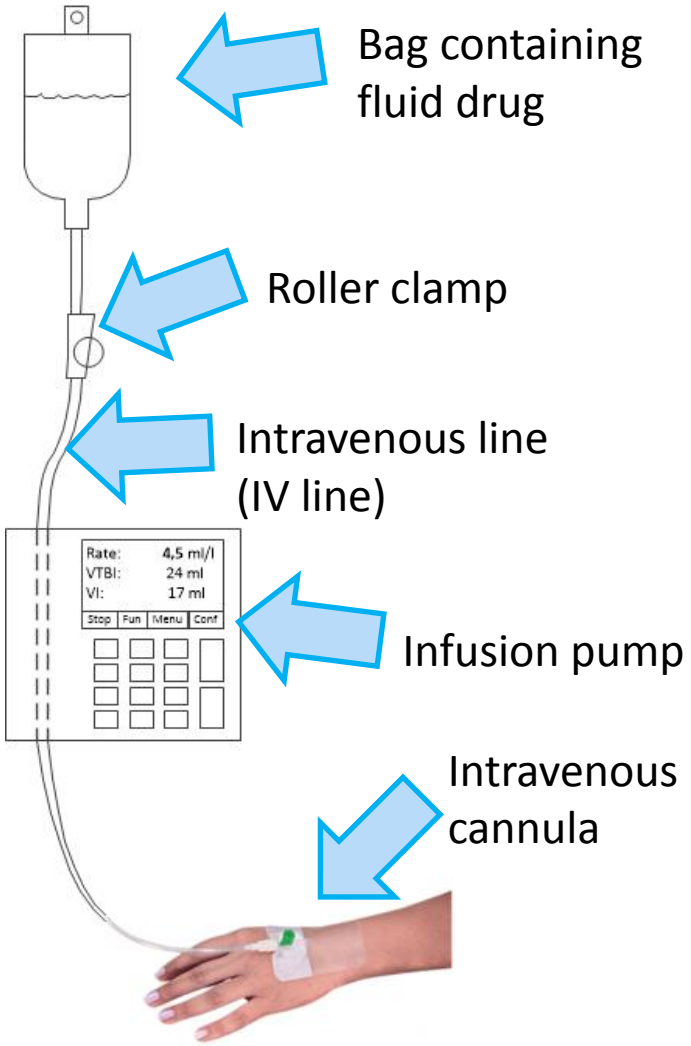
Zarządzanie zmianami

- Proces zarządzania zmianami dotyczy wszystkich artefaktów w cyklu życia systemu, argumentacji też!
- Zmiany argumentacji dotyczą przede wszystkim dowodów

Cel:

- zapewnić spójność zmian dowodów w argumentacji wiarygodności (*assurance case*)

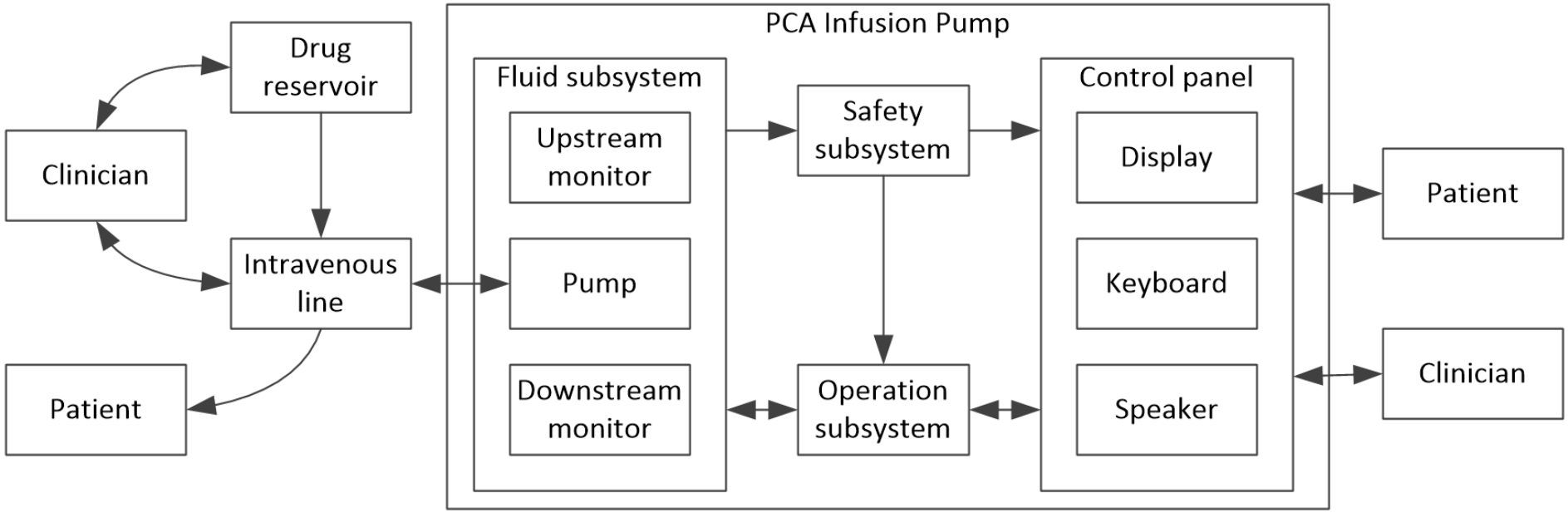
System: Pompa infuzyjna



source: www.wikipedia.org

Model systemu PCA Infusion Pump

- System obejmuje:
  - oprogramowanie
  - elementy elektryczne i mechaniczne
  - ludzi (pacjent i personel medyczny)
- System jest zdefiniowany w notacji AADL



źródło: B. R. Larson, J. Hatcliff: *Open Patient-Controlled Analgesia Infusion Pump System Requirements*, Draft 0.11, SAnToS TR 2014-6-1, Kansas State University, 2014

Modelowanie

Wpływ zmiany elementu na inne elementy analizowany jest w kontekście konkretnej perspektywy

Przykłady perspektyw:

- struktura systemu
- cykl życia
- technologia
- przepływ sterowania lub danych
- położenie fizyczne
- struktura argumentacji

Przykład perspektywy struktury systemu

			Parent	Dependencies
Users		S1		
	Patient	S2	S1	S6, S14
	Clinician	S3	S1	S5, S6, S14
Infusion set		S4		
	Drug reservoir	S5	S4	S3, S6
	Intravenous line	S6	S4	S1, S5, S8
PCA Infusion Pump		S7		
	Fluid subsystem	S8	S7	S6, S12, S13
		upstream monitor	S9	S8	
		pump	S10	S8	
		downstream monitor	S11	S8	
	Operation subsystem	S12	S7	S8, S13, S14
	Safety subsystem	S13	S7	S8, S12, S14
	Control panel	S14	S7	S2, S3, S12, S13
		Display	S15	S14	
		Keyboard	S16	S14	
		Speaker	S17	S14	

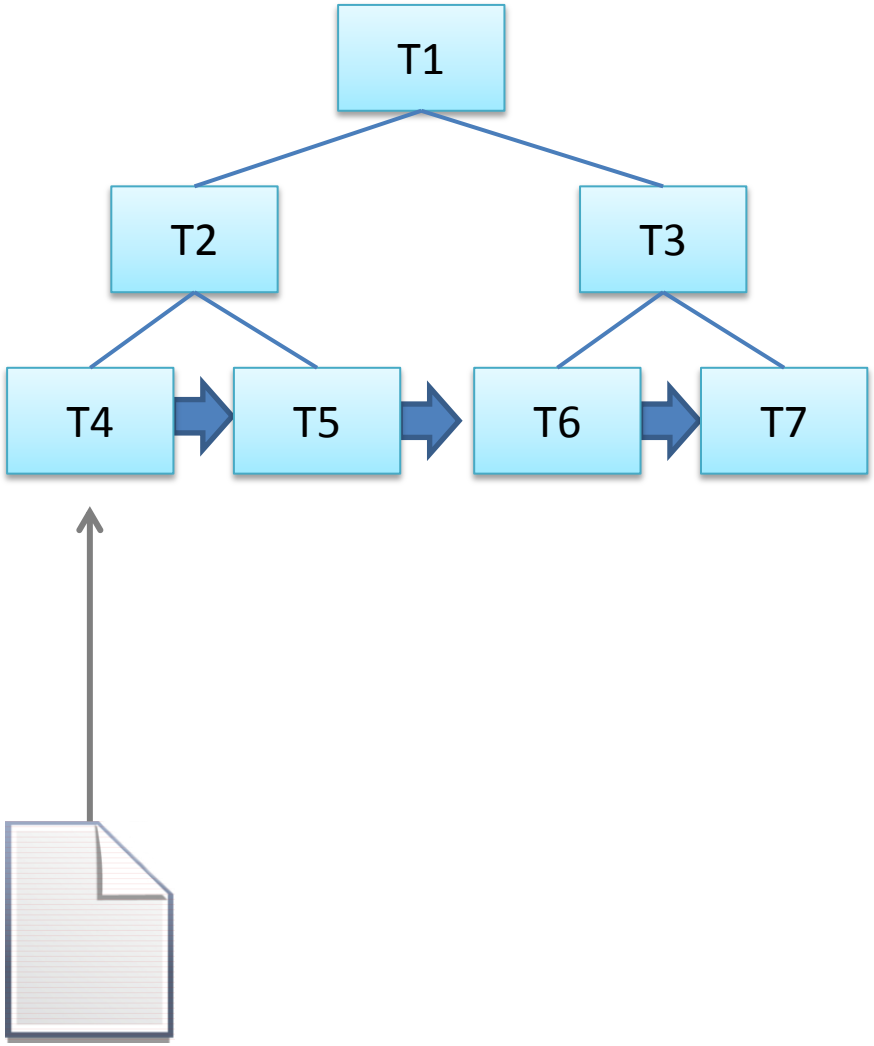
Model ogólny

Dla perspektywy definiujemy:

- hierarchię
- relacje wpływu

Dowód jest przypisany

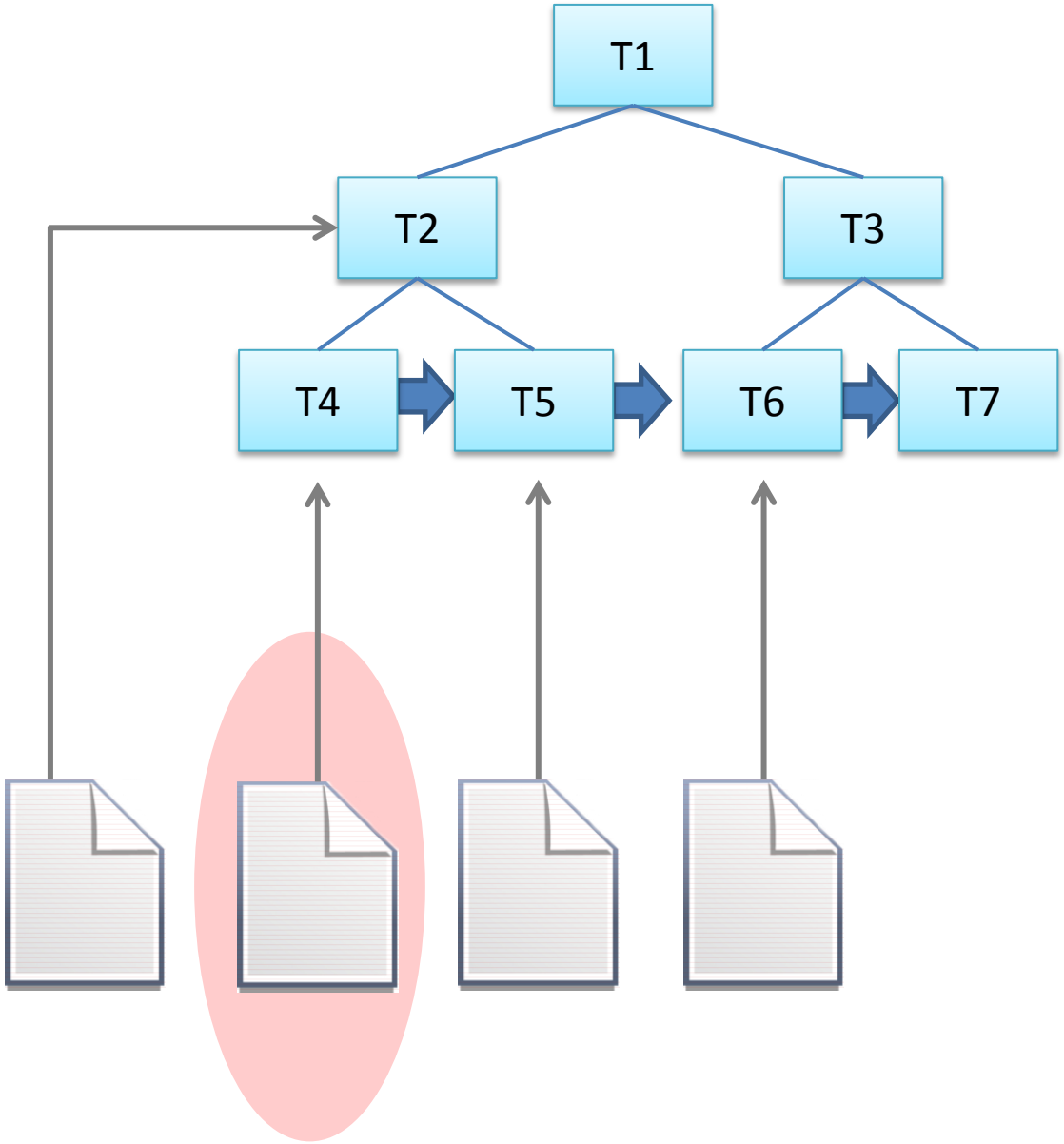
do elementu perspektywy



Krok 1. identyfikacja pierwotnej zmiany

Punktem startowym jest zmiana jednego dowodu

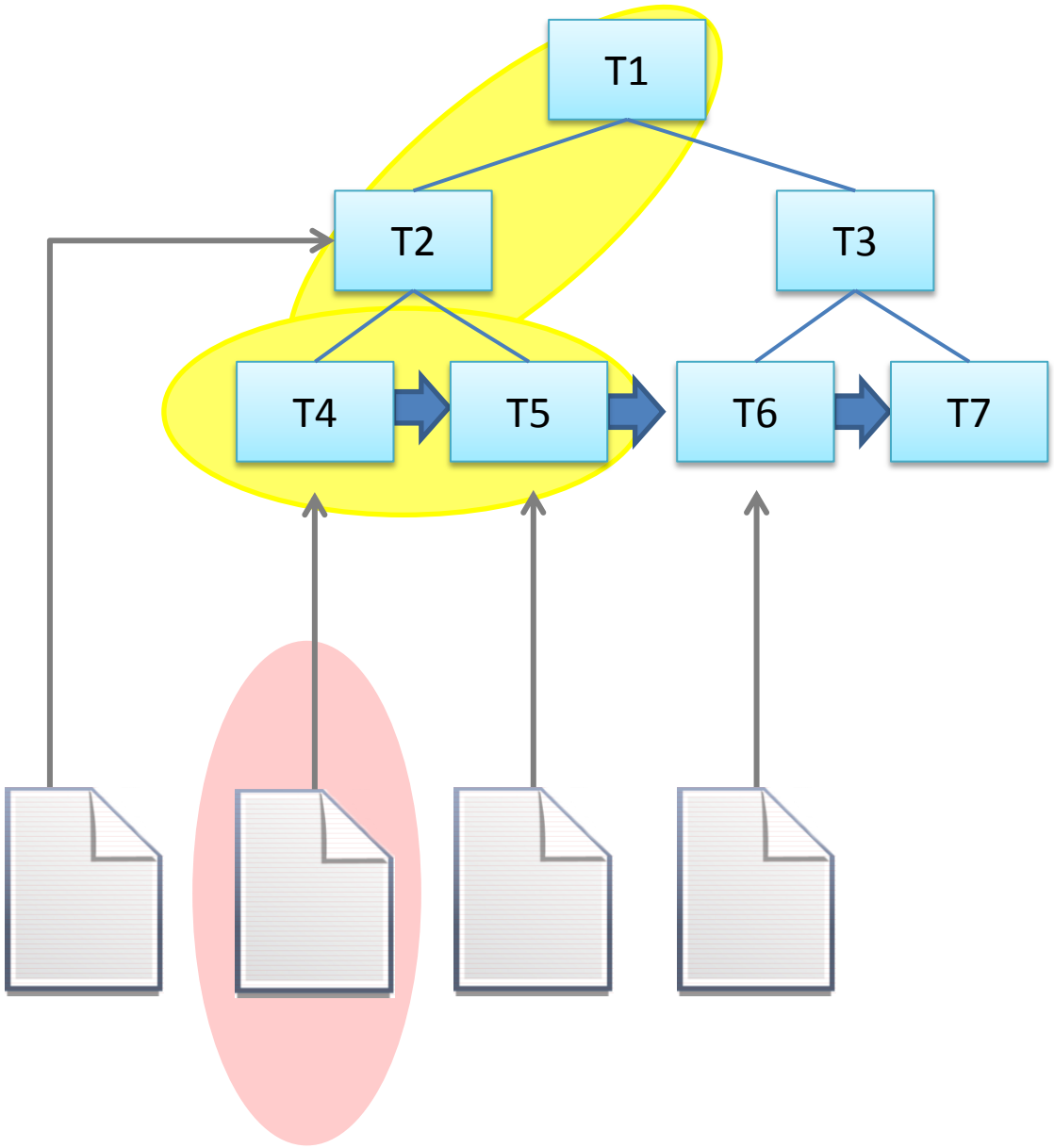
Zakładamy, że dowody są przypisane do elementów perspektyw



Krok 2. Określenie zakresu wpływu

Propagacja zmiany może następować:

- w jednej lub wielu perspektywach w wymiarze hierarchii
- w jednej perspektywie w relacji wpływu

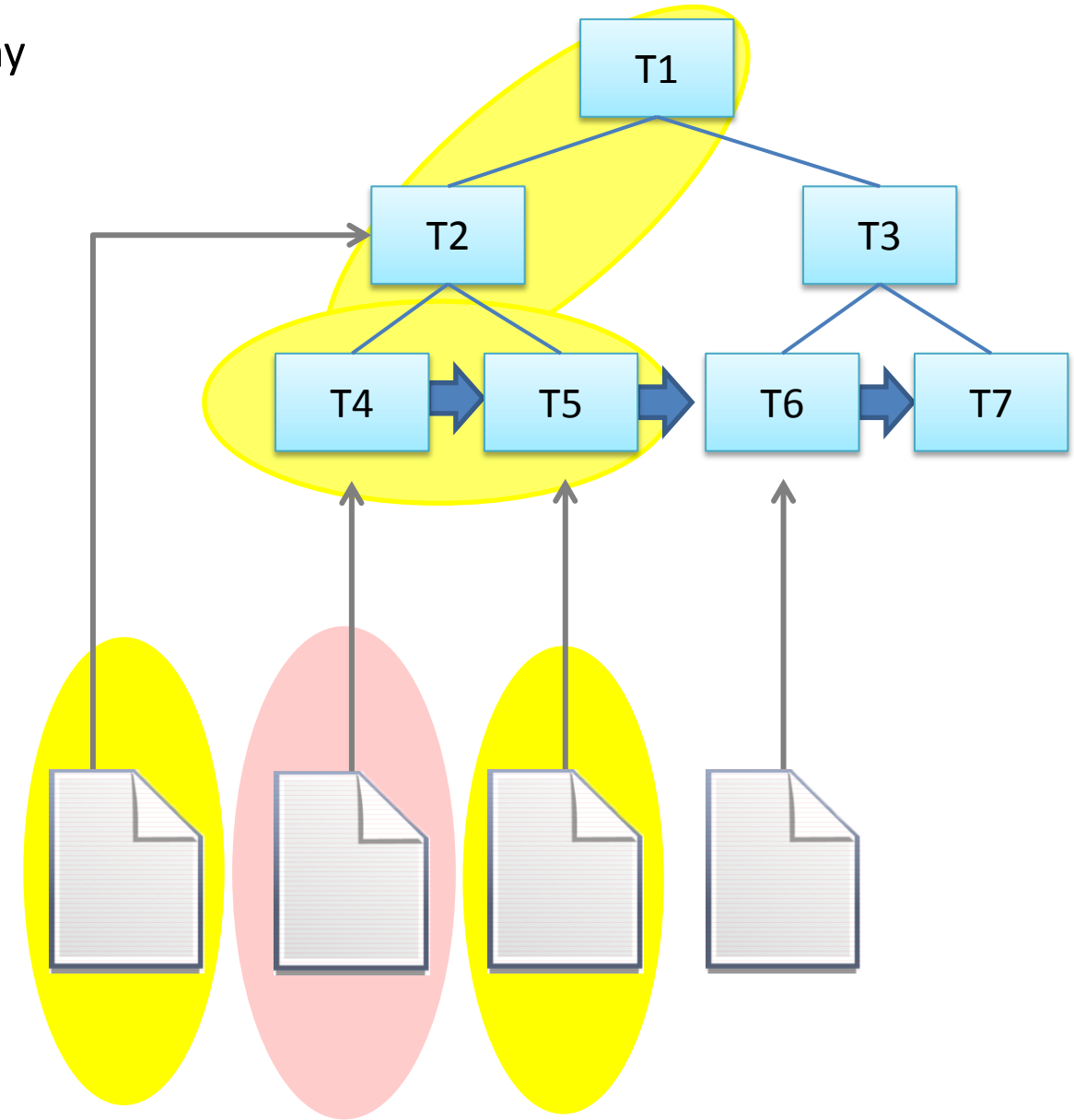


Krok 3. Identyfikacja zakresu wpływu

Każdy dowód w zakresie zmiany podlega ocenie:

- czy zmiana pierwotna wymusza modyfikację
- czy modyfikacja nie jest wymagana

Jeżeli wymagana jest modyfikacja, powtarzane są kroki 1-3 dla danego dowodu.



Analiza hazardu: powietrze w linii

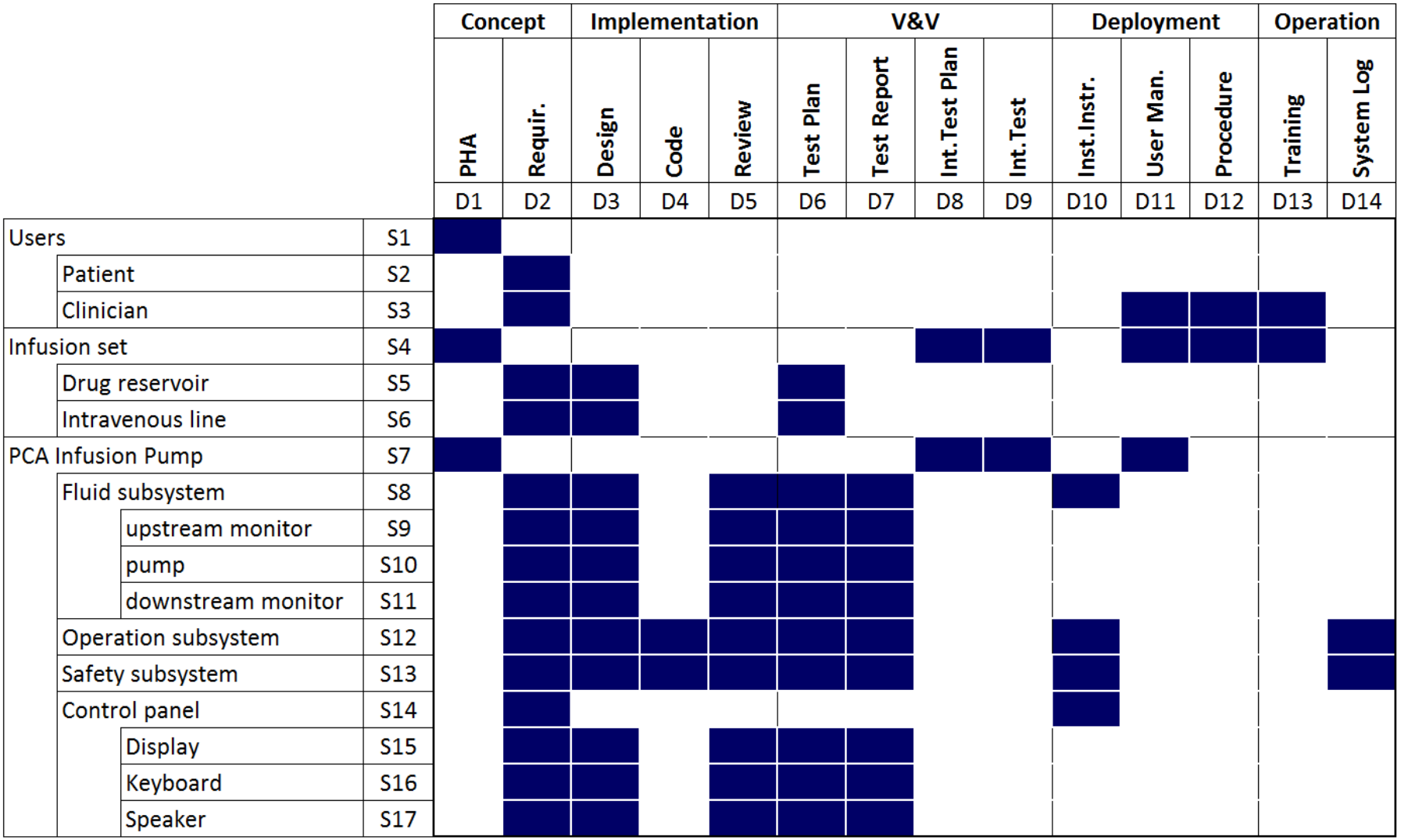
Ogólna struktura argumentacji:

- system jest bezpieczny, gdy ryzyko hazardów jest na akceptowalnym poziomie
  - hazardy są akceptowane, gdy stosowane są skuteczne zabezpieczenia
    - Skuteczne zabezpieczenia obejmują prewencję, wykrywanie i naprawę
      - Zabezpieczenie jest skuteczne, gdy spełnione są wynikające wymagania bezpieczeństwa

Preventive controls	**Detective controls**	**Corrective controls**
Clinician training mitigates external sources of air in line Clinician manual and training ensures: - compatible infusion set - sealed delivery path - expelling air from line	Downstream monitor detects air bubbles	Alarm sound and displayed message Pumping halted Failure recorded in the log

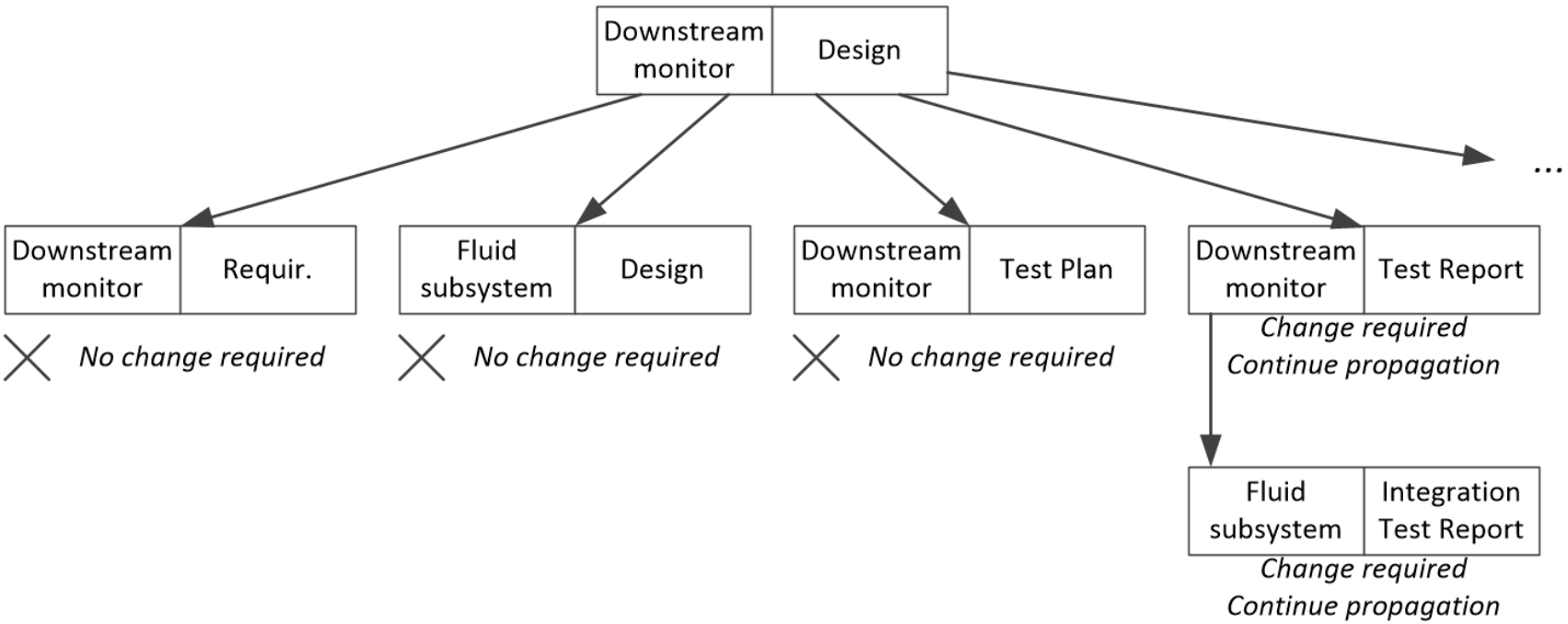
Evidence framework

Macierz dowodów dla argumentacji pompy PCA



Zmiana 1: bez zmiany interfejsu

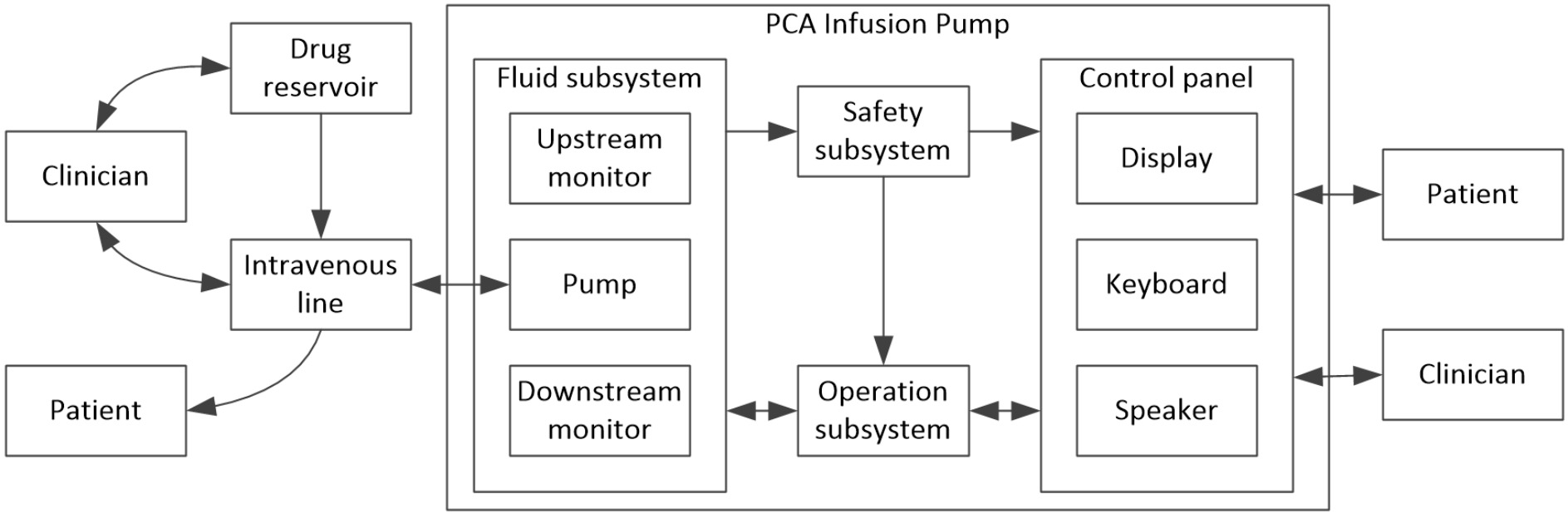
Zmiana 1: zmiana czujnika na element od innego producenta z zachowaniem zgodności interfejsów



Evidence matrix

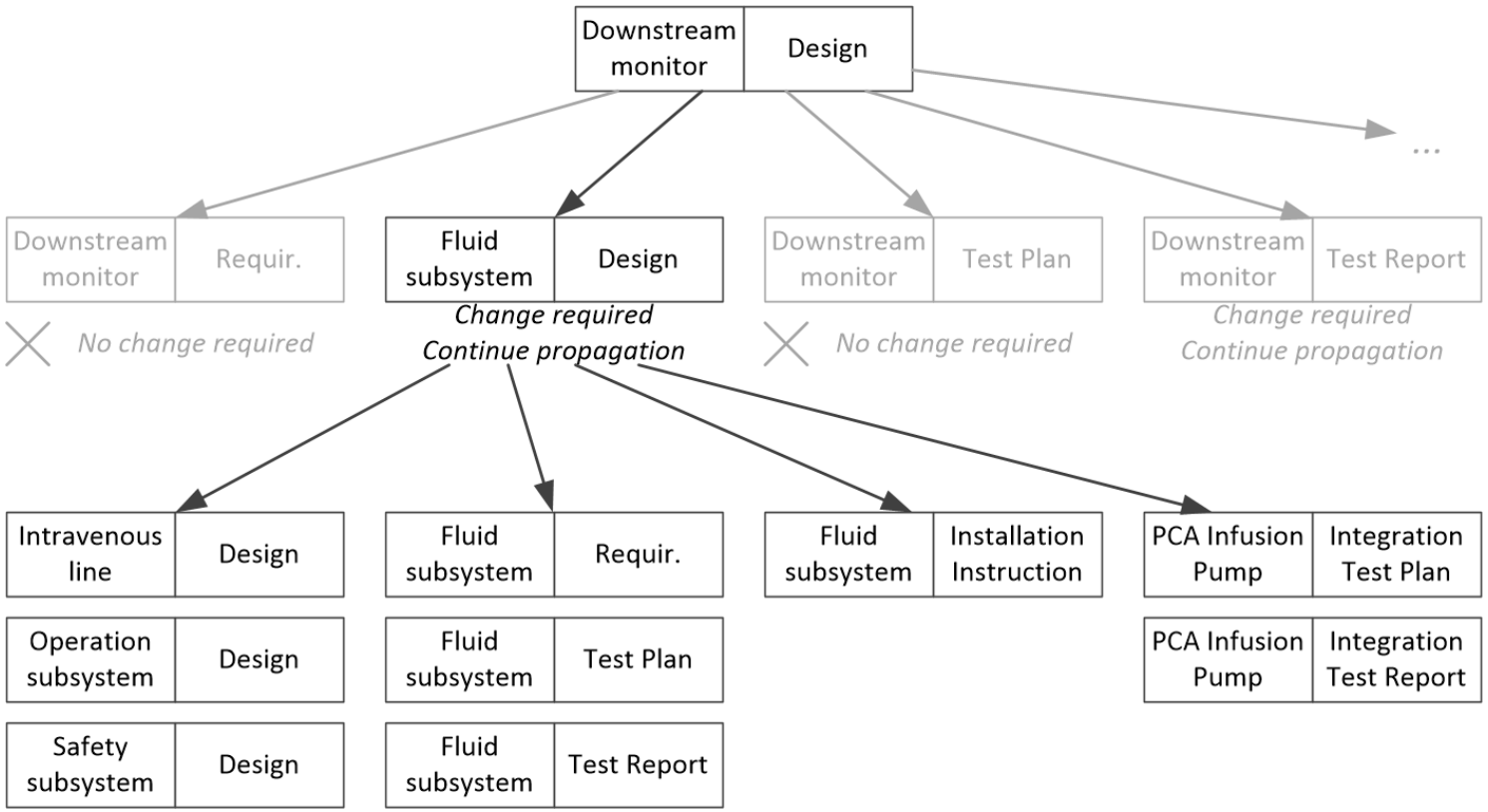
		Concept		Implementation			V&V				Deployment			Operation	
		PHA	Requir.	Design	Code	Review	Test Plan	Test Report	Int.Test Plan	Int.Test	Inst.Instr.	User Man.	Procedure	Training	System Log
		D1	D2	D3	D4	D5	D6	D7	D8	D9	D10	D11	D12	D13	D14
Users	S1	■													
Patient	S2		■												
Clinician	S3		■									■	■	■	
Infusion set	S4	■							■	■		■	■	■	
Drug reservoir	S5		■	■			■								
Intravenous line	S6		■	■			■								
PCA Infusion Pump	S7	■							v	3		■			
Fluid subsystem	S8		■	v		3	v	3			v				
upstream monitor	S9		■	■		■	■	■							
pump	S10		■	■		■	■	■							
downstream monitor	S11		v	1		2	v	2							
Operation subsystem	S12		■	■	■	■	■	■			■				■
Safety subsystem	S13		■	■	■	■	■	■			■				■
Control panel	S14		■								■				
Display	S15		■	■		■	■	■							
Keyboard	S16		■	■		■	■	■							
Speaker	S17		■	■		■	■	■							

Dla przypomnienia…

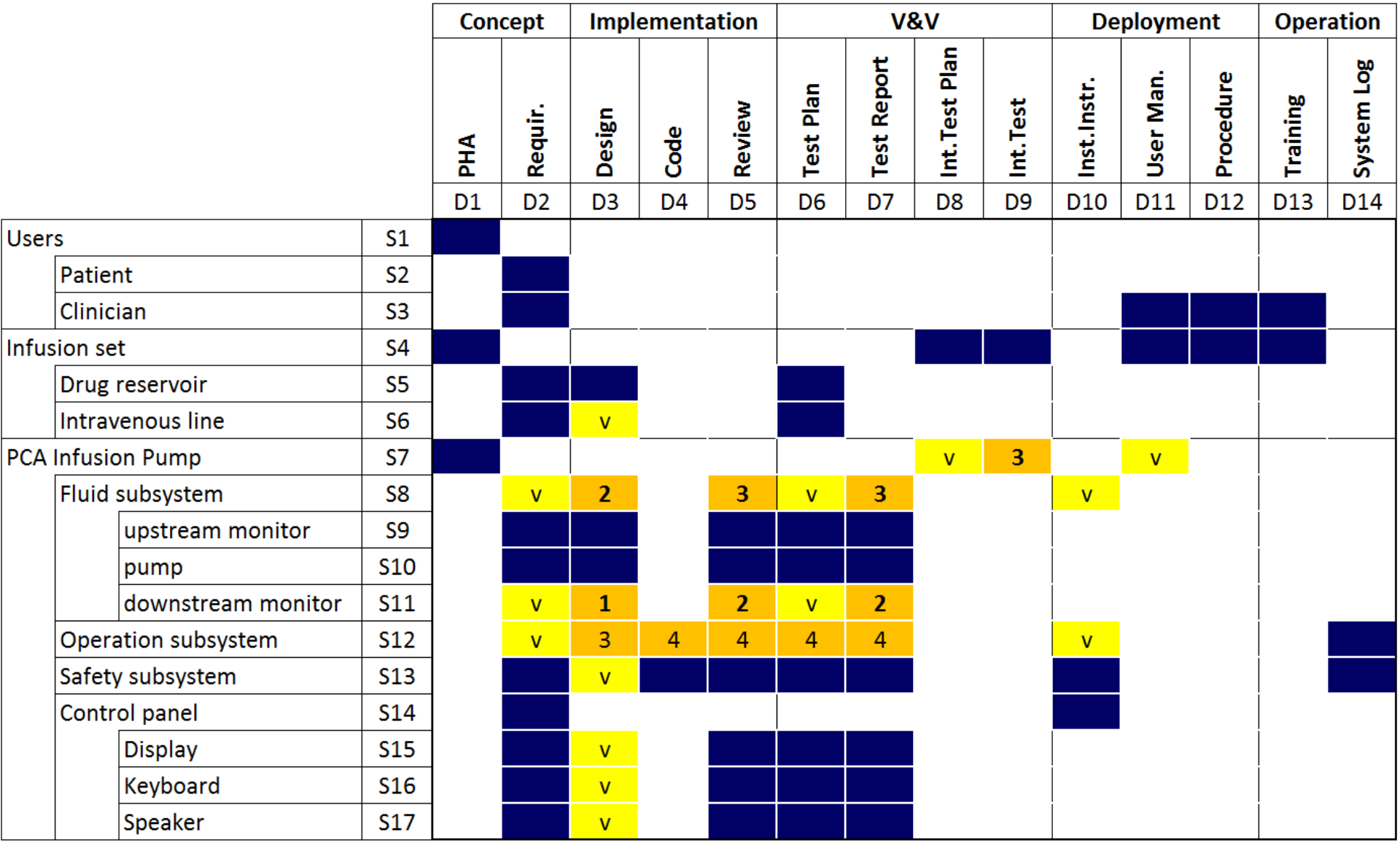


Zmiana 2: zmiana interfejsu czujnika

Zmiana 2: zmiana czujnika na element od innego producenta ze zmianą interfejsu



Zakres wpływu zmiany 2



Profil zmiany

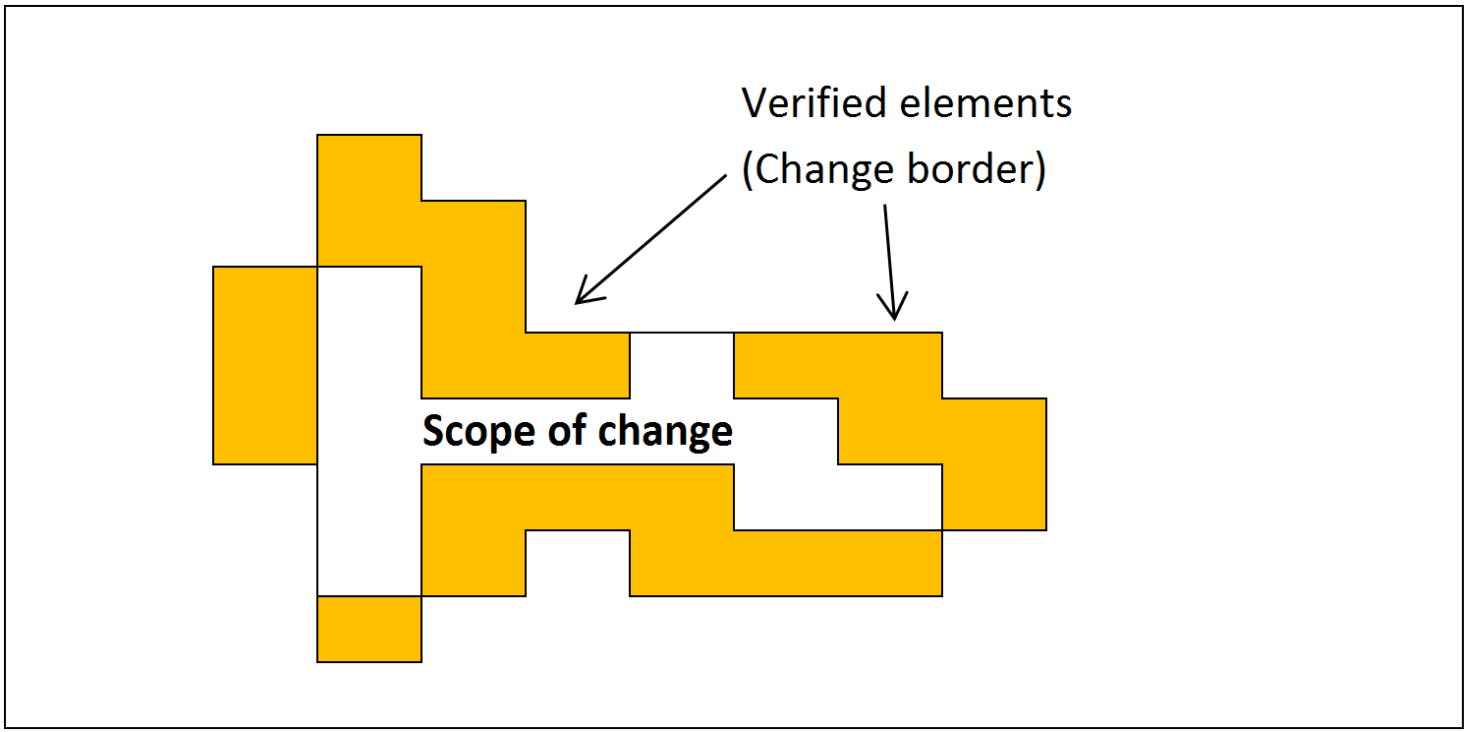
W wyniku analizy wpływu zmiany można podzielić dowody na trzy kategorie:

- podlegające zmianie
- zweryfikowane jako niewymagające zmiany (granica zmiany)
- poza zakresem zmiany

Mapa wymienionych trzech kategorii tworzy profil zmiany.

Profil poprawnej analizy zmian zachowuje spójność – nie wszystkie kombinacje są legalne.

Znając jakie dowody są modyfikowane można określić, czy profil zachowuje spójność



Podsumowanie

- Dowody w argumentacji wiarygodności powinny być traktowane jako spójny zbiór powiązanych elementów
- Pierwsze eksperymenty (bez narzędzia) wskazują, że skuteczne jest opisywanie dowodów z użyciem:
  - hierarchicznych tagów z relacjami wpływu
- Opracowany algorytm analizy wpływu zmiany
  - ocena wpływu na dany element jest wykonywana przez człowieka
- Zmiana może być opisana przez profil zmiany w macierzy dowodów
  - profil zmiany ma określone warunki spójności – jest możliwe wykrywanie niespójnych zakresów wpływu zmiany
- Dalsze prace
  - rozszerzenie NOR-STA o tagi i analiza dla większych systemów
  - analiza zakresu zmian w strukturze argumentacji
  - zmiany struktury *evidence framework*