

WYBRANE ASPEKTY DOWODZENIA BEZPIECZEŃSTWA APLIKACJI

Przemysław Ilczuk ¹, Dariusz Szmel ²

¹ Politechnika Warszawska, Wydział Transportu, ² Badacz niezależny

XV KONFERENCJA NAUKOWO-TECHNICZNA „PROJEKTOWANIE, BUDOWA I UTRZYMANIE
INFRASTRUKTURY W TRANSPORCIE SZYNOWYM” INFRASZYN 2023

26-28.04.2023, ZAKOPANE



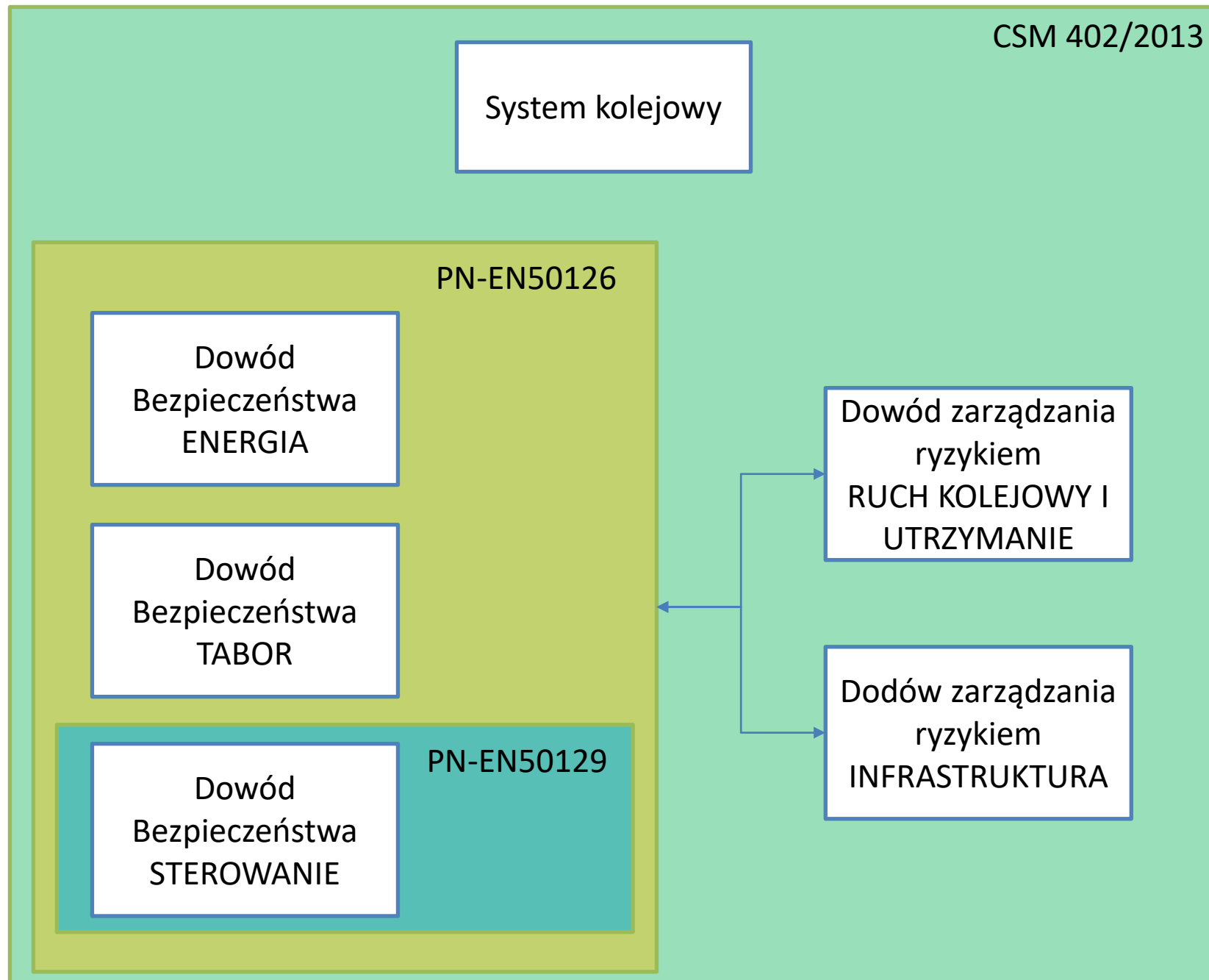
**Ośrodek
Certyfikacji
Transportu**

NA WYDZIALE TRANSPORTU
POLITECHNIKI WARSZAWSKIEJ

Normy CENELEC

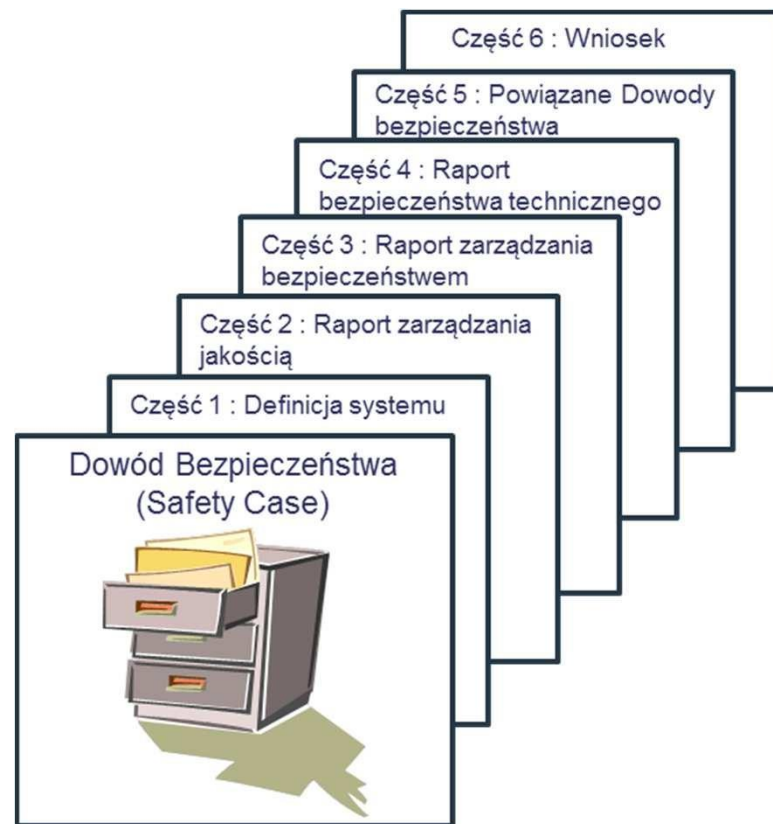
- **PN-EN 50126 cz 1. i 2**
 - pojęcia RAMS, model „V”, specyfikacja wymagań RAMS, system zarządzania bezpieczeństwem, (ogólny) Dowód Bezpieczeństwa
 - zastosowanie do SRK, ENE i Pojazdów
- **PN-EN 50129**
 - bezpieczeństwo elektronicznych urządzeń srk, (szczegółowy) Dowód Bezpieczeństwa,
- **PN-EN 50128**
 - bezpieczeństwo oprogramowania
- **PN-EN 50159**
 - bezpieczeństwo systemów transmisyjnych



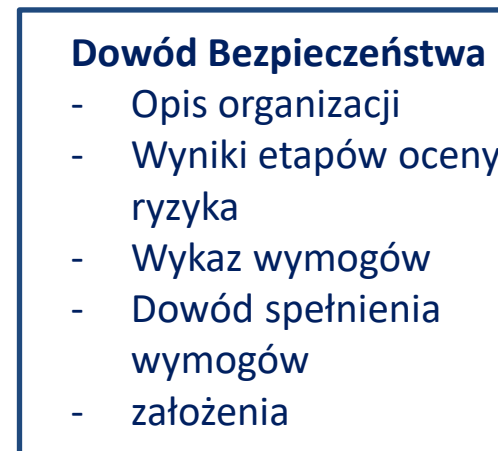


Dowód bezpieczeństwa

Dowód bezpieczeństwa to zbiór ok. 80-100 różnych dokumentów
Dokument o tytule „Dowód bezpieczeństwa” to usystematyzowany przewodnik po w/w zbiorze



Struktura Dowodu Bezpieczeństwa według normy PN-EN50126 i PN-EN50129



Struktura Dowodu stosowania procesu zarządzania ryzykiem według CSM 402/2013 (Załącznik 1, ust. 5.2)



1. Definicja rozpatrywanego systemu:

- kluczowe podsystemy/urządzenia;
- architektura i oczekiwane zachowanie;
- interfejsy i środowisko eksploatacji;
- wymogi bezpieczeństwa;
- definicja konfiguracji/wersji rozpatrywanego systemu, do której odnosi się przypadek bezpieczeństwa;
- odniesienie do wejściowych wymagań bezpieczeństwa, jak również związanych z nimi analiz oceny ryzyka.

2. Sprawozdanie z zarządzania jakością:

- działania i dowody w zakresie zarządzania jakością.

3. Raport o zarządzaniu bezpieczeństwem:

- działania i dowody w zakresie zarządzania bezpieczeństwem

4. Raport bezpieczeństwa technicznego:

- zapewnienie bezpieczeństwa w warunkach bezawaryjnych;
- zapewnienie bezpieczeństwa w przypadku awarii i błędów;
- zapewnienie bezpieczeństwa przy niekorzystnym wpływie czynników zewnętrznych;
- Warunki zastosowania związane z bezpieczeństwem (SRAC).

5. Powiązane dowody bezpieczeństwa:

- odniesienia do dowodów bezpieczeństwa wszystkich podsystemów/urządzeń, od których zależy główny przypadek bezpieczeństwa.
- wykazanie, że wszystkie warunki zastosowania związane z bezpieczeństwem określone w każdym z powiązanych podsystemów/sprzętu dowodów bezpieczeństwa są albo spełnione w głównym dowodzie bezpieczeństwa, albo przeniesione do dalszych warunków zastosowania związanych z bezpieczeństwem.

6. Wniosek:

- Podsumowanie dowodów przedstawionych w poprzednich częściach sprawy dotyczącej bezpieczeństwa;
- wykaz wszystkich szczególnych oświadczeń dotyczących bezpieczeństwa, oraz
- oświadczenie, że rozpatrywany system jest odpowiednio bezpieczny, pod warunkiem spełnienia określonych warunków stosowania.



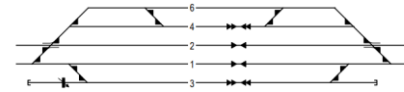
Etapy tworzenia dowodu bezpieczeństwa



Dowód
bezpieczeństwa
Produktu
GPSC



Dowód
bezpieczeństwa
Ogólnego
Zastosowania
GASC



Dowód
bezpieczeństwa
Określonego
Zastosowania
SASC



SASC
Application Design

SASC
Physical
Implementation



GPSC –Generic Product Safety Case

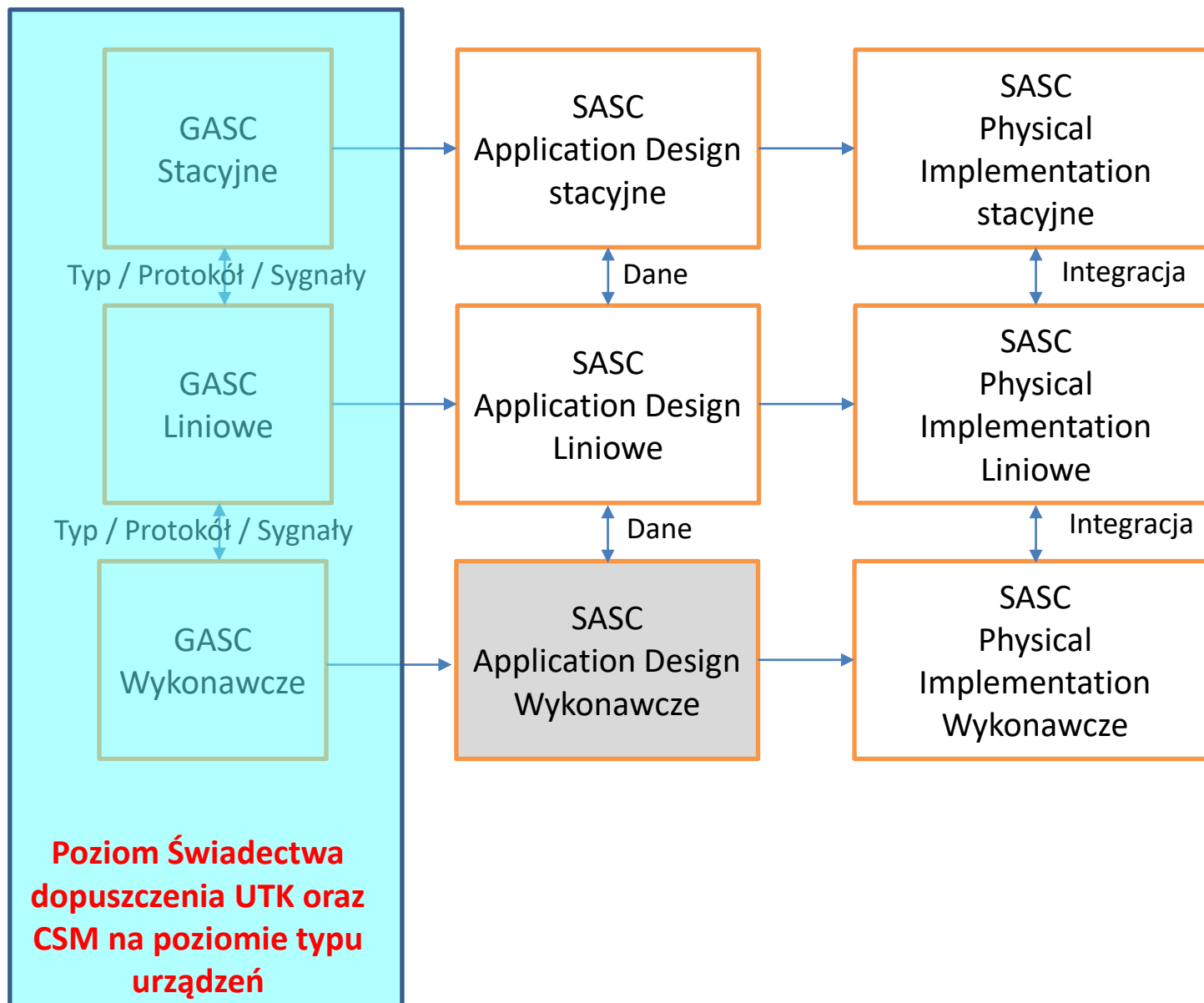
GASC –Generic Application Safety Case

SASC –Specific Application Safety Case

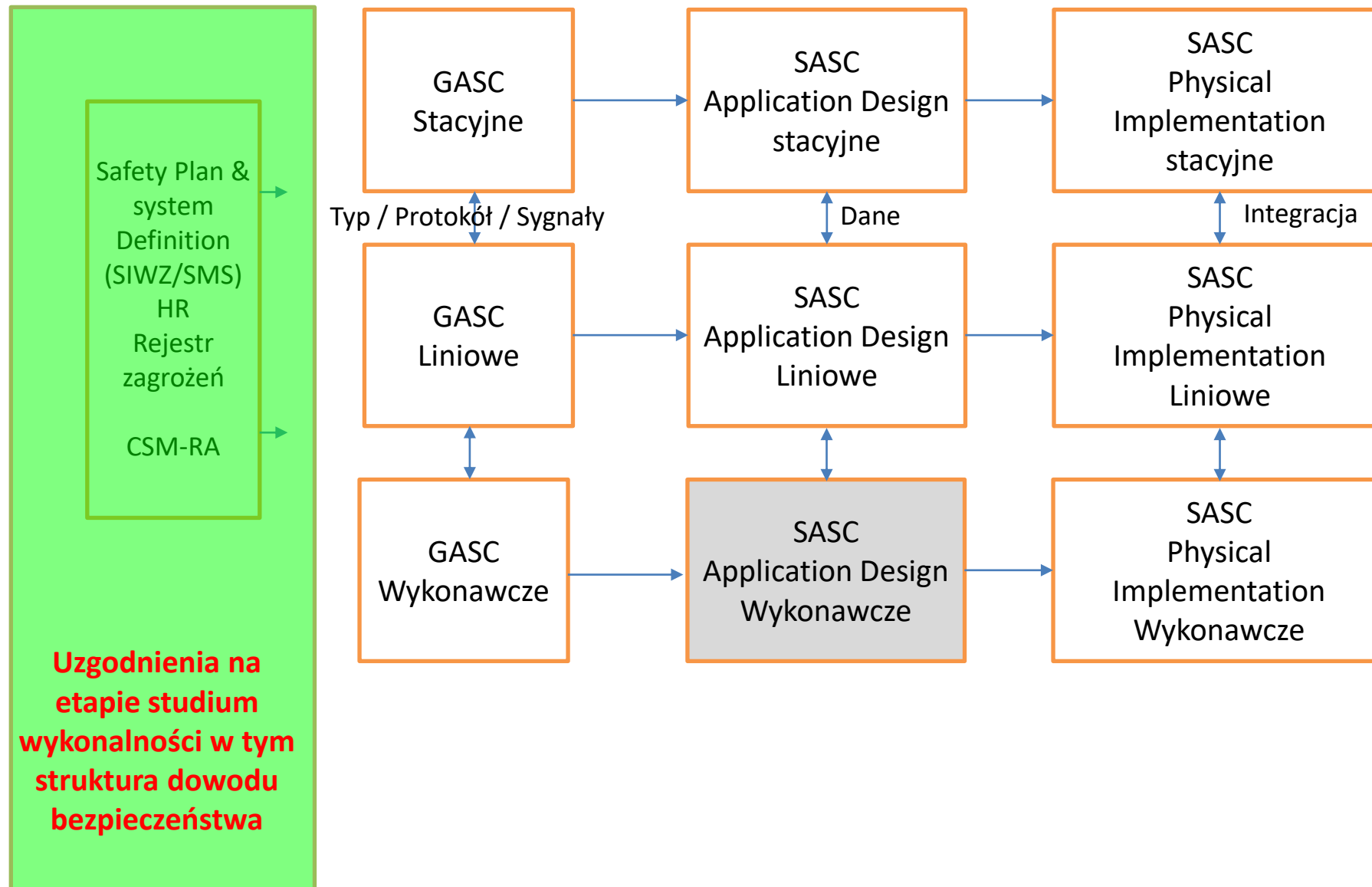


Etapy tworzenia dowodu bezpieczeństwa

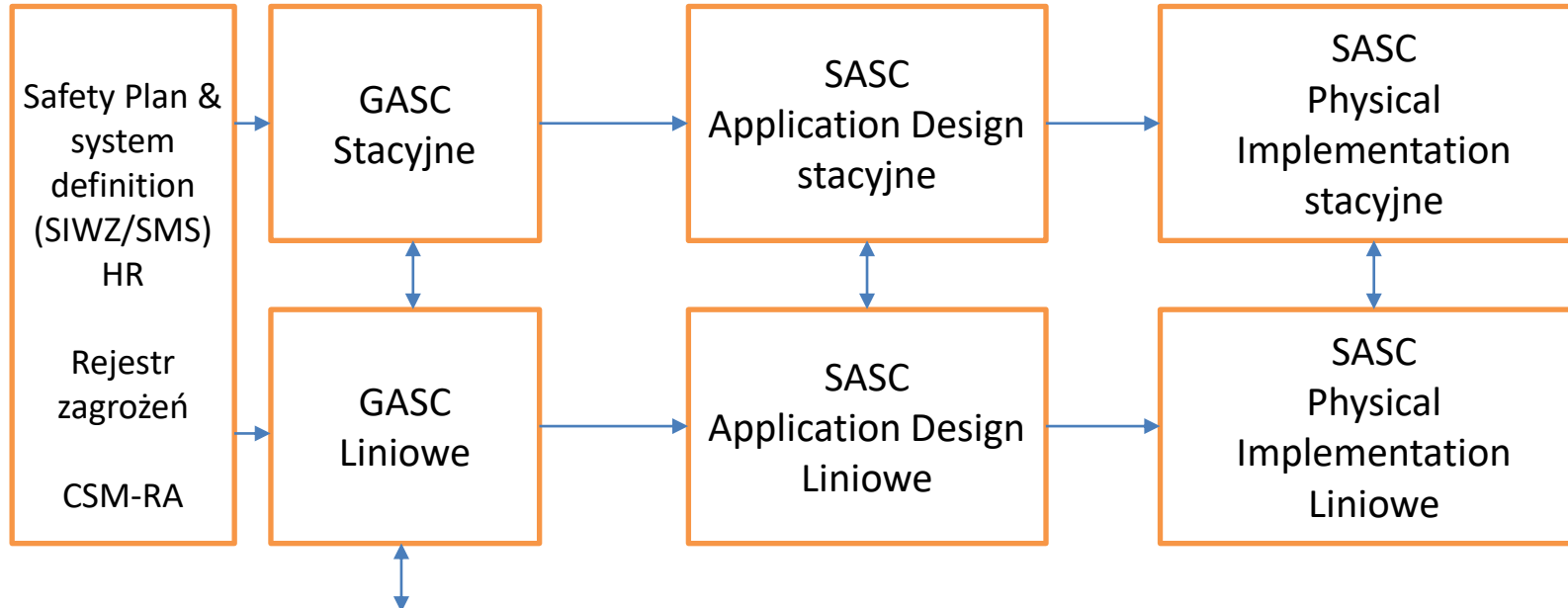
Przykładowy podział struktury dowodu bezpieczeństwa dla zadania inwestycyjnego



Etapy tworzenia dowodu bezpieczeństwa



Etapy tworzenia dowodu bezpieczeństwa

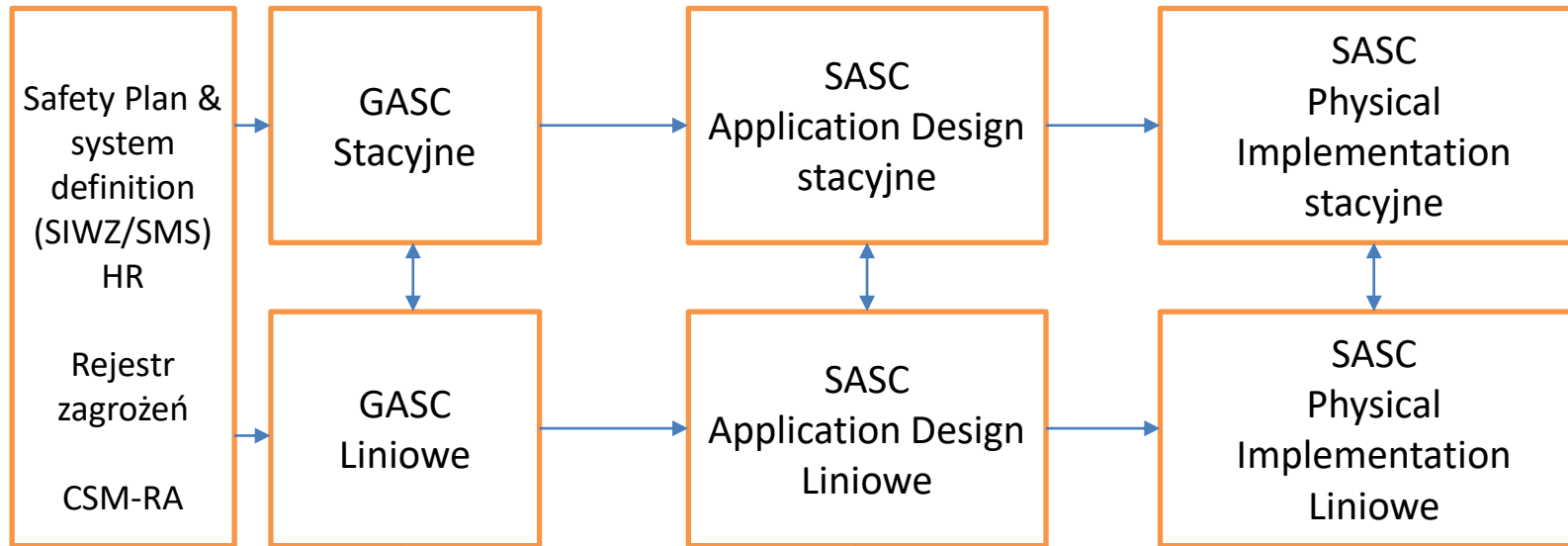


- FFR/HR/RAM
- WTWiO (instrukcje)
- Program szkoleniowy
- Definicja Interfejsów
- System SW i HW oraz interfejsy
- Spełnienie SRAC
- Przekazanie SRAC
- ISA
- Certyfikat typu
- Świadectwo



Etapy tworzenia dowodu bezpieczeństwa

10



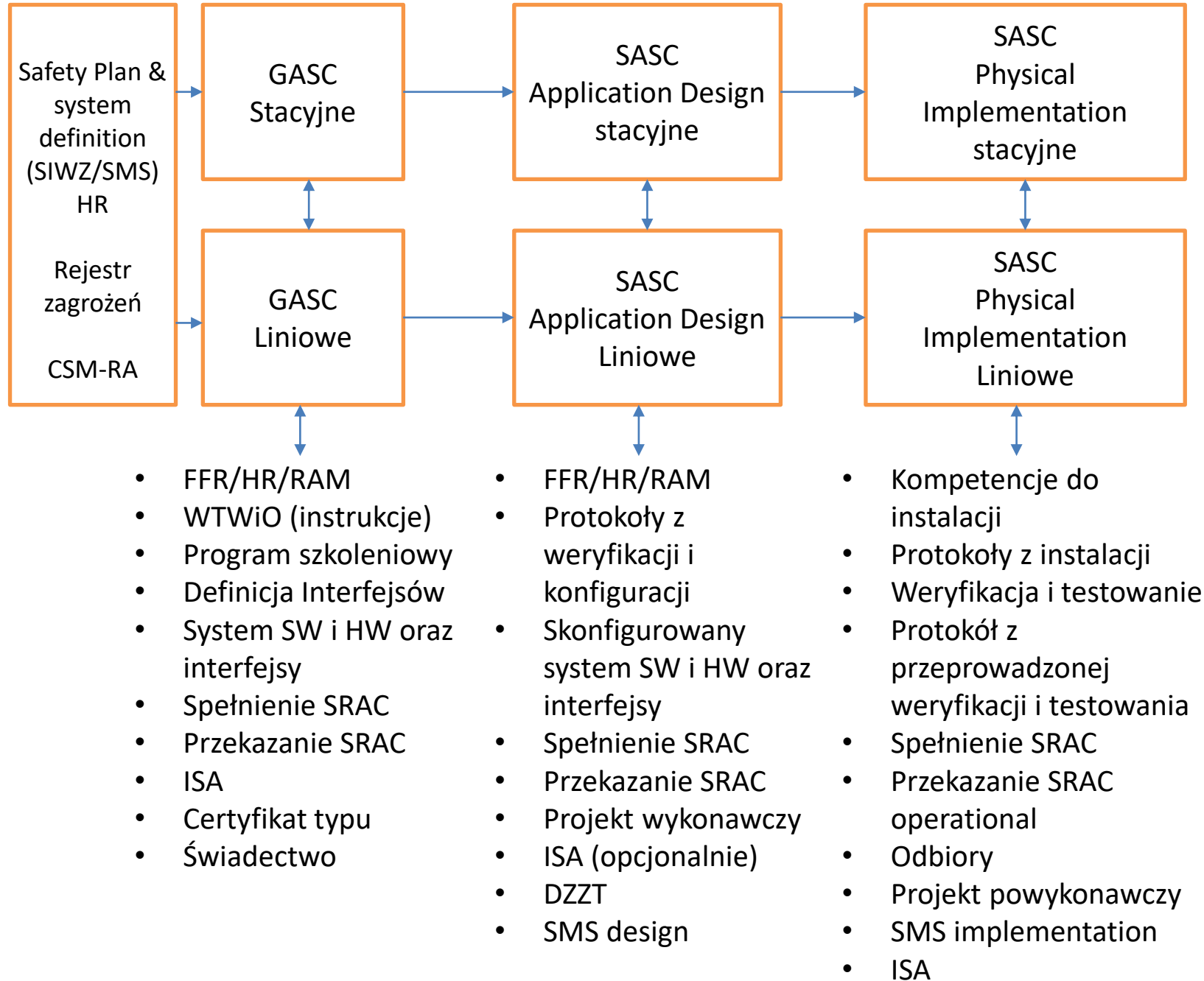
- FFR/HR/RAM
- WTWiO (instrukcje)
- Program szkoleniowy
- Definicja Interfejsów
- System SW i HW oraz interfejsy
- Spełnienie SRAC
- Przekazanie SRAC
- ISA
- Certyfikat typu
- Świadectwo

- FFR/HR/RAM
- Protokoły z weryfikacji i konfiguracji
- Skonfigurowany system SW i HW oraz interfejsy
- Spełnienie SRAC
- Przekazanie SRAC
- Projekt wykonawczy
- ISA (opcjonalnie)
- DZZT
- SMS design



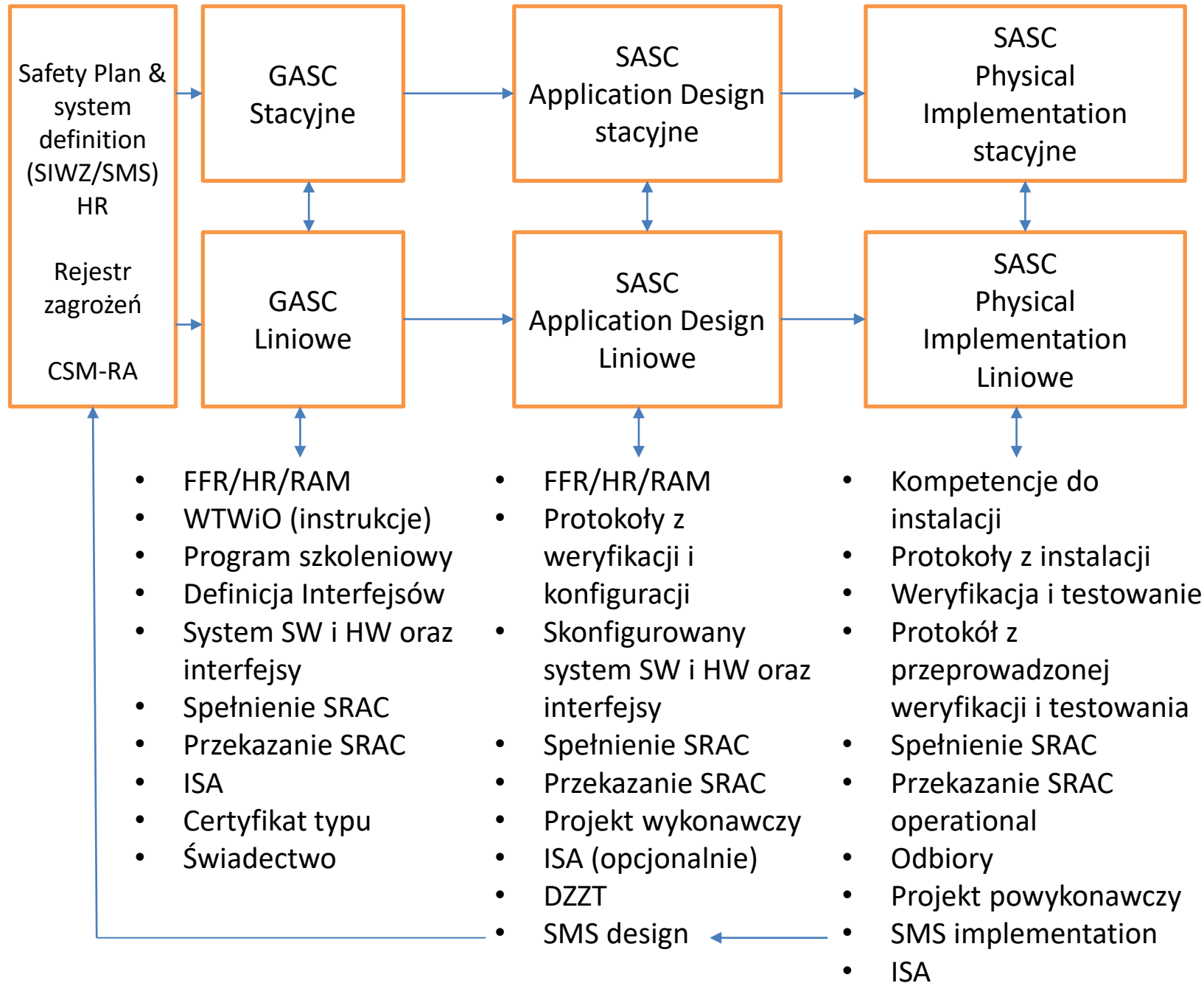
Etapy tworzenia dowodu bezpieczeństwa

11



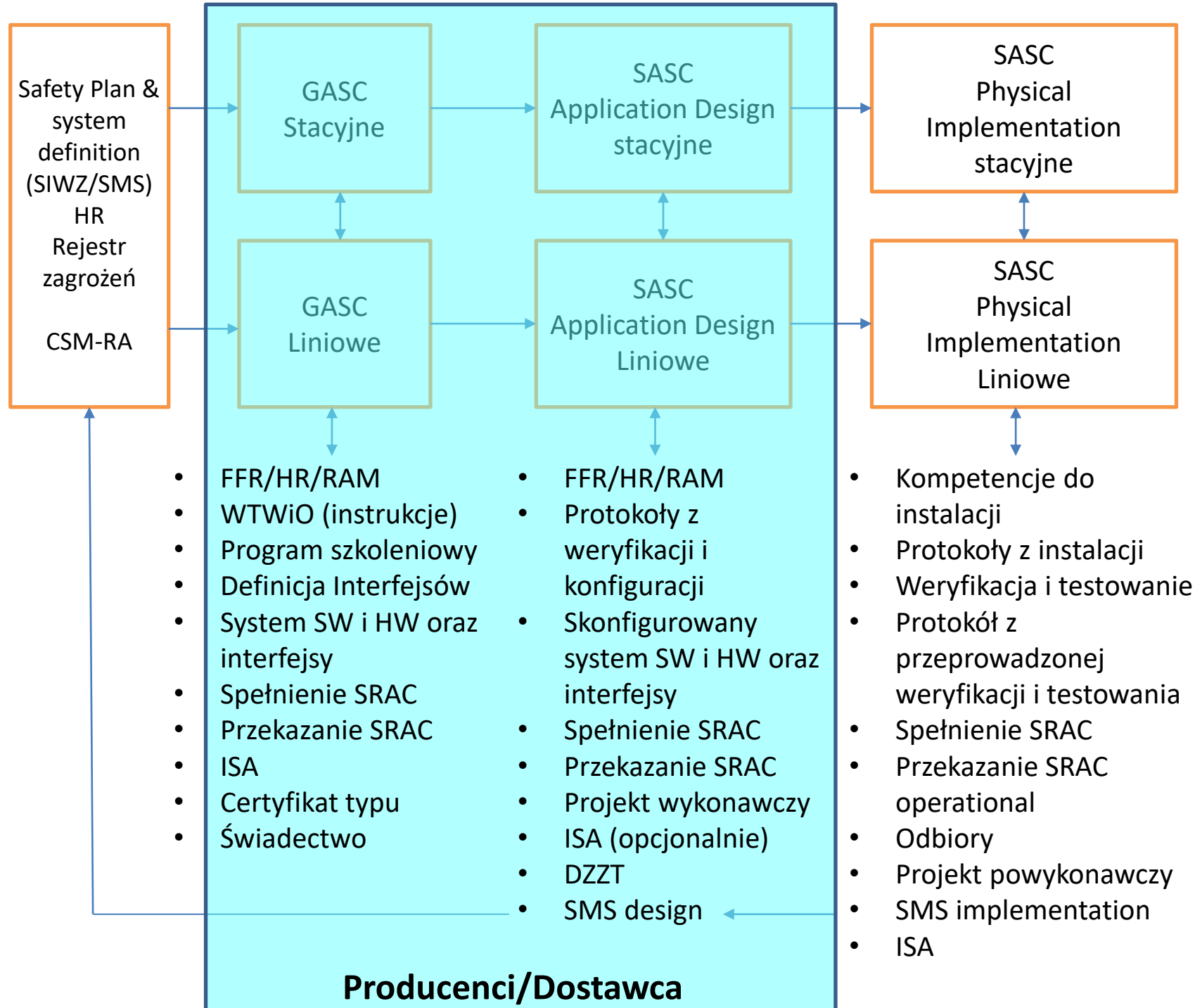
Etapy tworzenia dowodu bezpieczeństwa

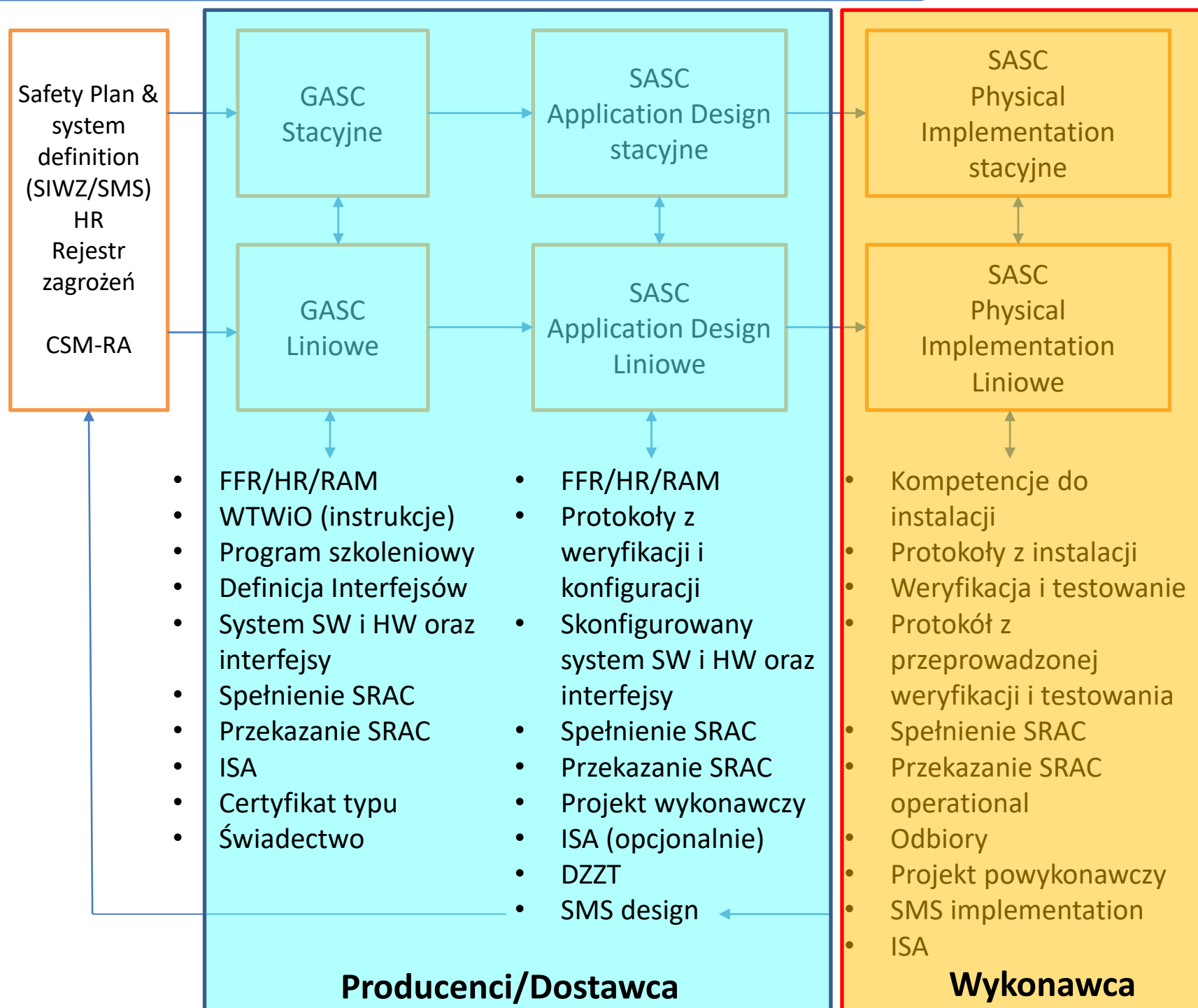
12

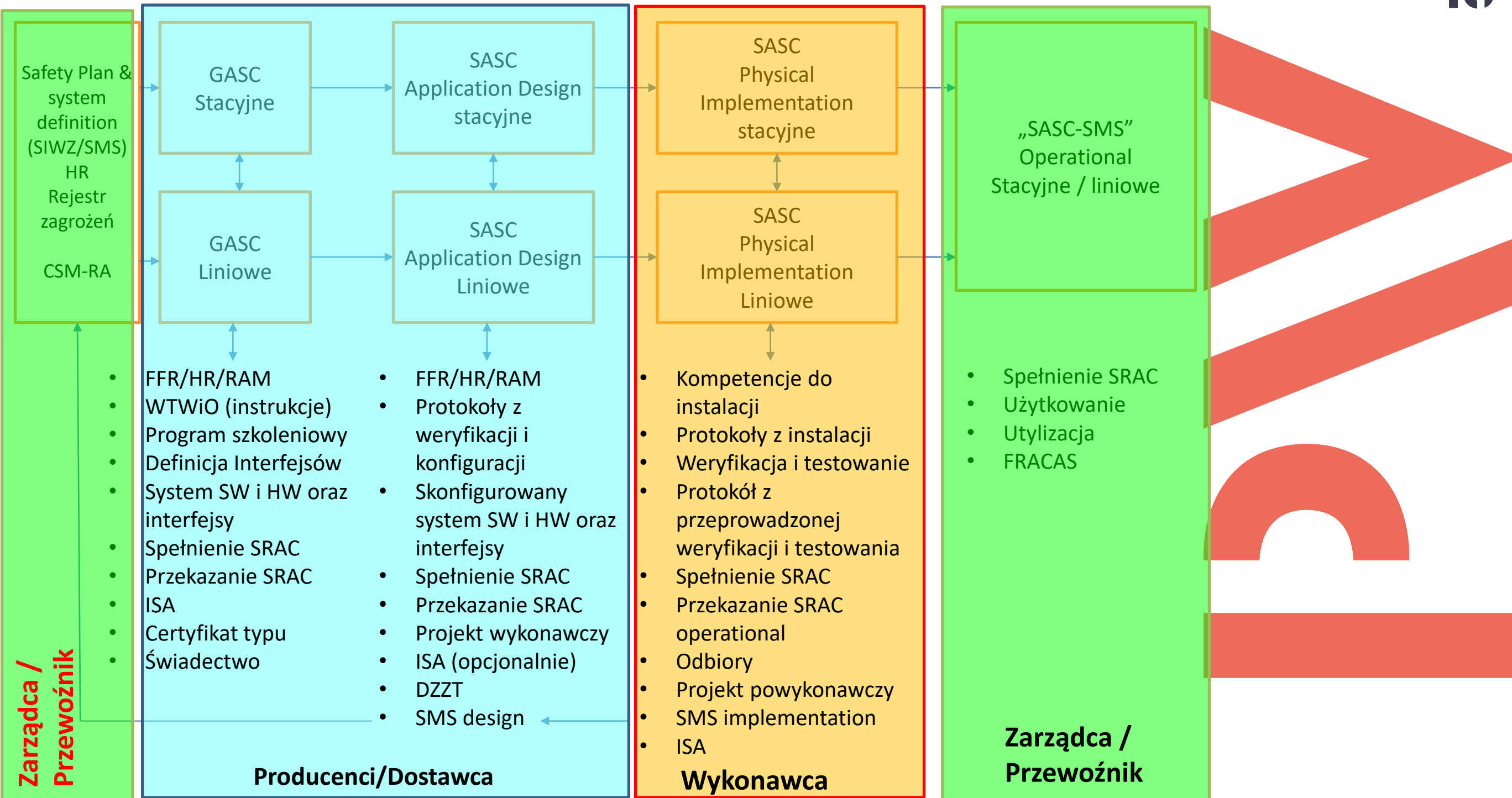


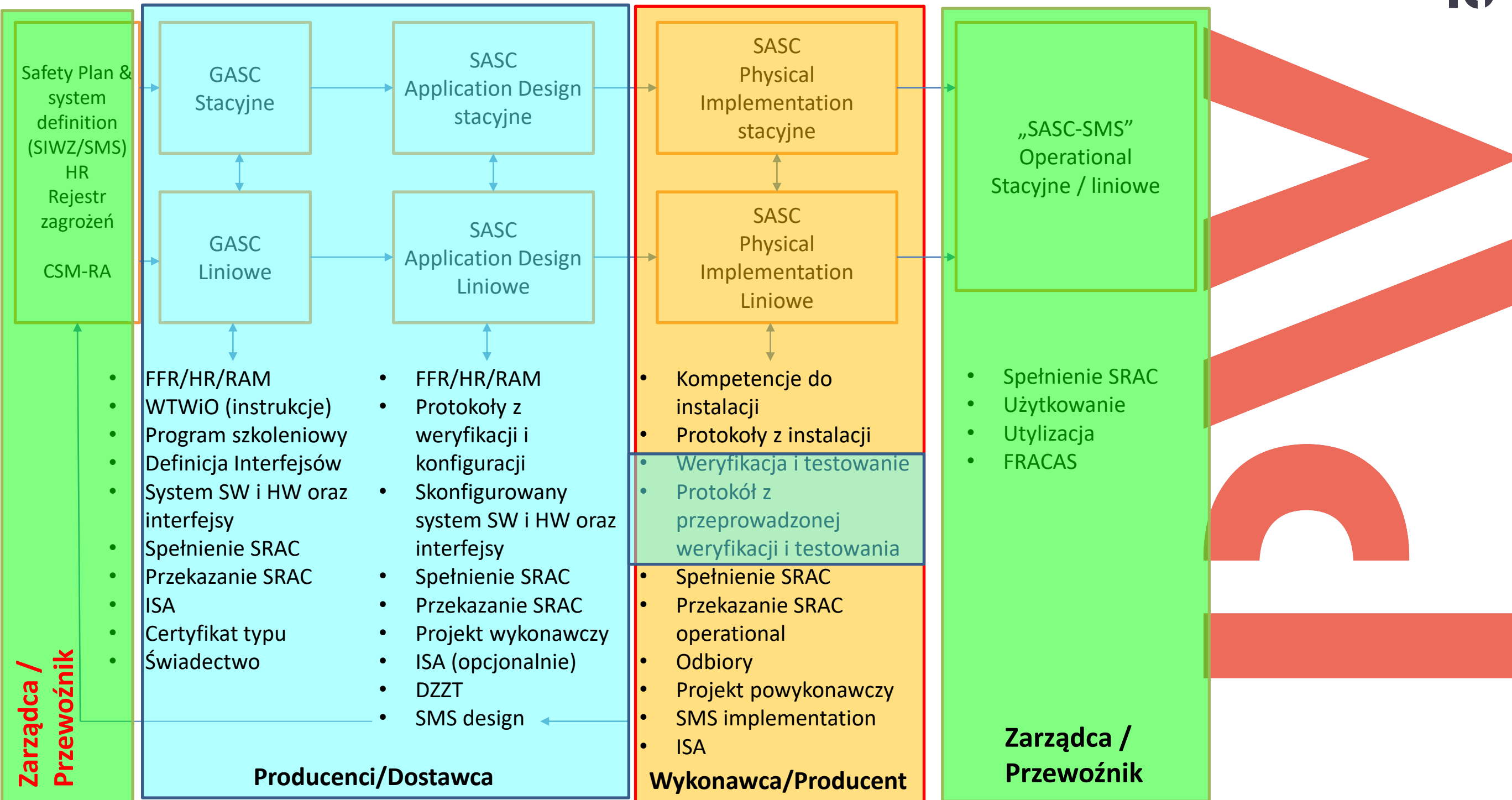
Etapy tworzenia dowodu bezpieczeństwa

13



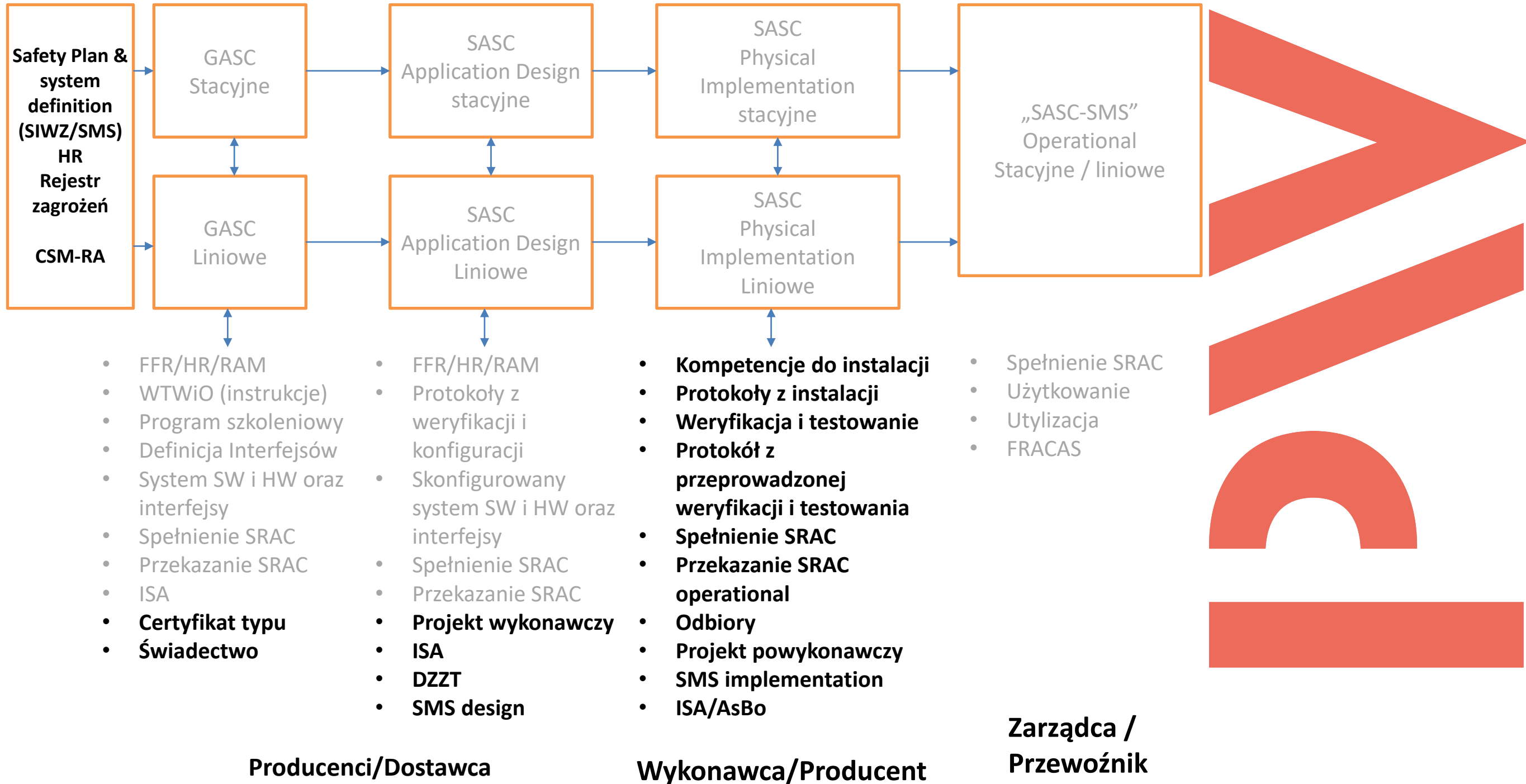






DOWÓD BEZPIECZEŃSTWA PODSYSTEMU

17



Dziękujemy za uwagę

Ilczuk Przemysław przemyslaw.ilczuk@pw.edu.pl
Dariusz Szmel dariusz.szmel@gmail.com

