Systemy zabezpieczeń

Definicja

System zabezpieczeń (*safety-related system*) jest to system, który implementuje funkcje bezpieczeństwa konieczne do utrzymania bezpiecznego stanu instalacji oraz jest przeznaczony do osiągnięcia koniecznej nienaruszalności bezpieczeństwa (*safety integrity*) tych funkcji.

- Funkcja bezpieczeństwa

Funkcja, przeznaczona do utrzymania bezpiecznego stanu instalacji w odniesieniu do konkretnego zdarzenia zagrażającego.

- Zdarzenie zagrażające

Sytuacja, której wynikiem jest fizyczny uraz lub pogorszenie stanu zdrowia ludzi, tak bezpośrednie jak pośrednie, wynikające ze szkody w majątku lub w środowisku

Uwagi

- może być integralną częścią systemu sterującego instalacją lub odrębnym systemem
- może być zaprojektowany do zapobiegania lub łagodzenia skutków zdarzenia zagrażającego
- może być realizowany w różnych technikach

Norma PN-EN 61508, listopad 2004 (IEC 61508)

Bezpieczeństwo funkcjonalne elektrycznych / elektronicznych / programowalnych elektronicznych systemów związanych z bezpieczeństwem

1: Wymagania ogólne
2: Wymagania dotyczące elektrycznych/elektronicznych/programowalnych systemów związanych z bezpieczeństwem
3: Wymagania dotyczące oprogramowania
4: Definicje i skrótowce
5: Przykłady metod do określania poziomów nienaruszalności i bezpieczeństwa
6: Wytyczne do stosowania
7: *Przegląd technik i miar*

Projektowanie bezpieczeństwa systemu

C — konsekwencje wystąpienia zdarzenia zagrażającego
P — prawdopodobieństwo wystąpienia zdarzenia

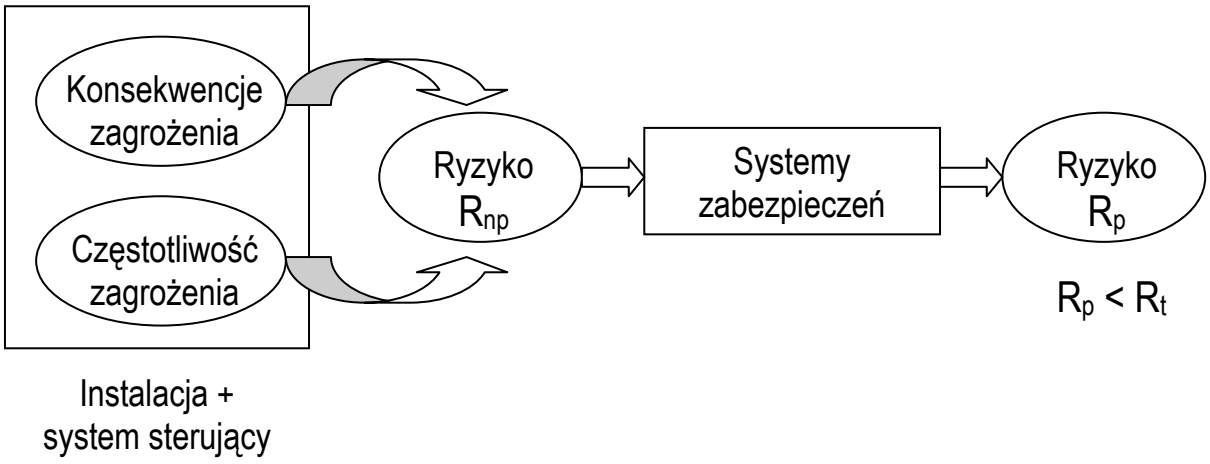
R — ryzyko związane ze zdarzeniem:

$$R = C \times P$$

1. Obliczyć ryzyko instalacji sterowanej bez zabezpieczeń R_{np}
2. Określić ryzyko dopuszczalne R_t
3. Jeśli $R_{np} > R_t$ to konieczna redukcja ryzyka w stopniu:

   $$PFD = F_t / F_{np}$$

4. Wprowadzić funkcje bezpieczeństwa (zabezpieczenia) o niezawodności PFD



Nienaruszalność bezpieczeństwa

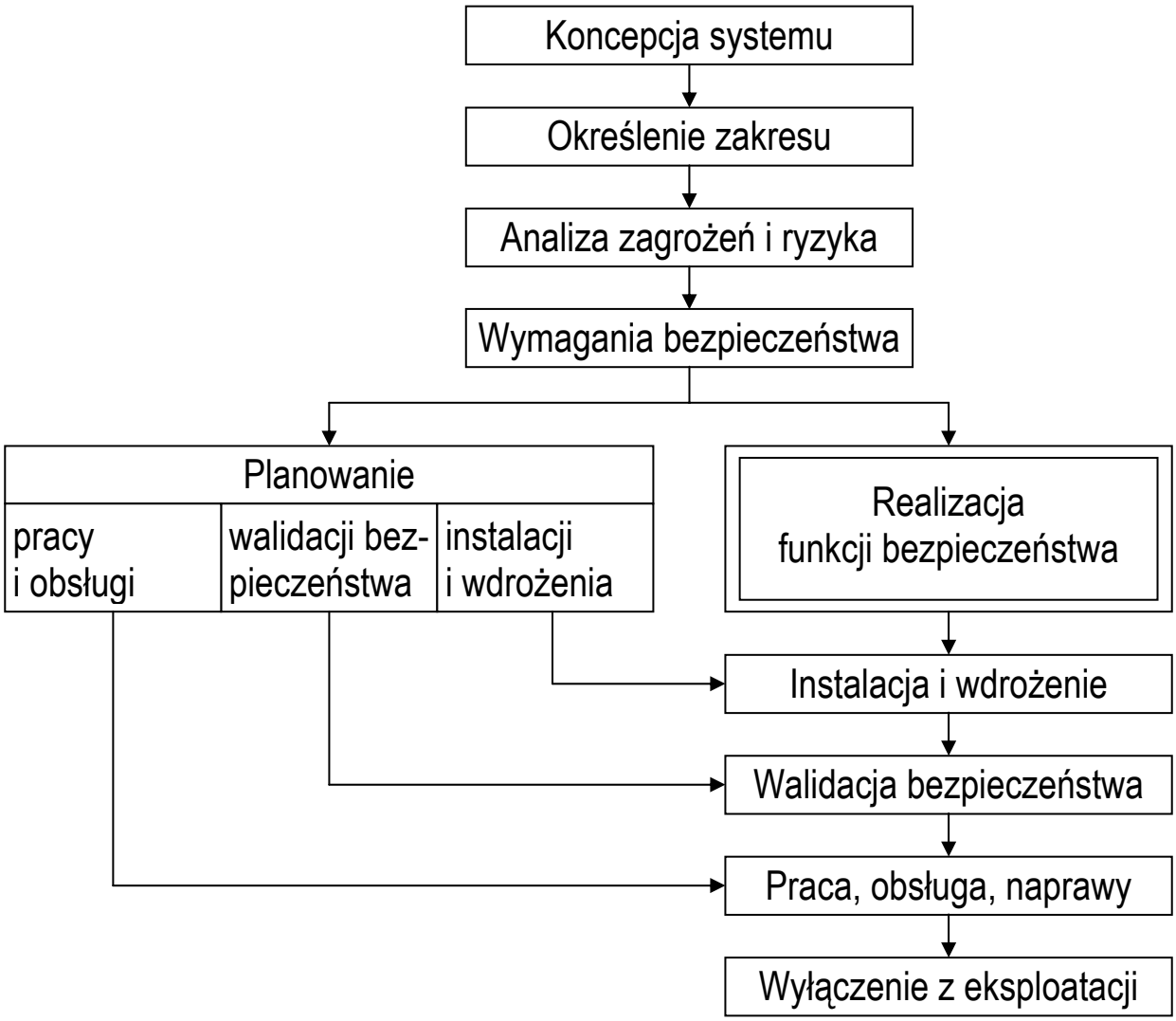
Prawdopodobieństwo, że system wykona wymagane funkcje bezpieczeństwa w zadanych warunkach i czasie.

- Rodzaje pracy
  - na rzadkie przywołanie: nie częściej niż raz na rok i nie częściej niż dwukrotność okresów testowych
  - na częste lub ciągłe przywołanie

- Poziomy nienaruszalności bezpieczeństwa (*SIL*)

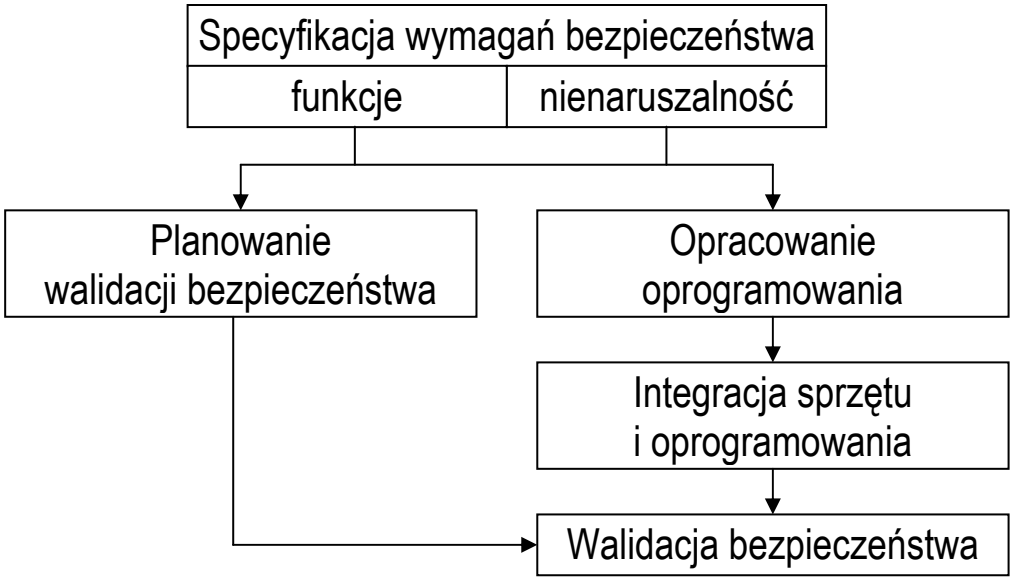
Poziom	Na rzadkie przywołanie (prawdopodobieństwo uszkodzenia)	Na częste przywołanie (prawd. uszkodzenia na godzinę)
4	10^{-5} ... 10^{-4}	10^{-9} ... 10^{-8}
3	10^{-4} ... 10^{-3}	10^{-8} ... 10^{-7}
2	10^{-3} ... 10^{-2}	10^{-7} ... 10^{-6}
1	10^{-2} ... 10^{-1}	10^{-6} ... 10^{-5}

Cykl utrzymania bezpieczeństwa

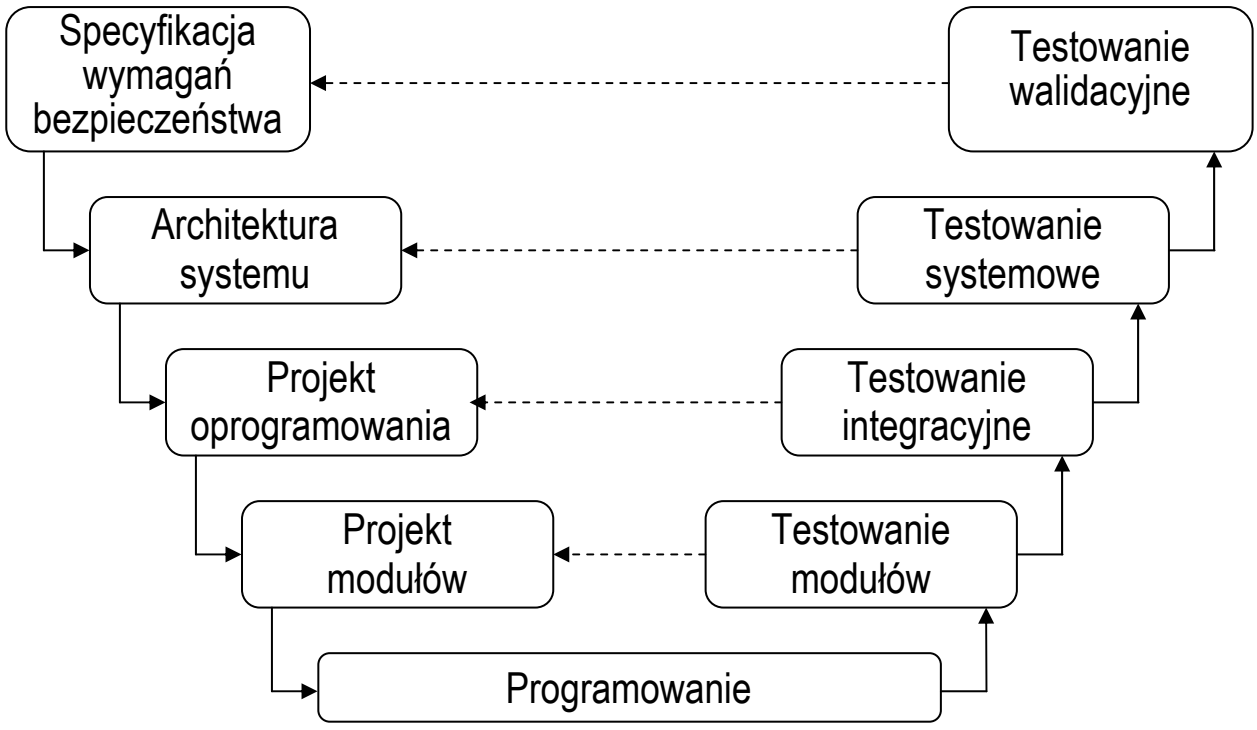


Wymagana dokumentacja wykonania wszystkich faz cyklu

Programowa realizacja funkcji bezpieczeństwa



- Cykl wytwarzania



Przykładowe rekomendacje normy

- Projektowanie architektury oprogramowania

	Technika/metoda	SIL1	SIL2	SIL3	SIL4
1	Wykrywanie i diagnoza defektów	–	R	HR	HR
2	Kody detekcyjne i korekcyjne	R	R	R	HR
3a	Blok odzyskiwania	R	R	R	R
3b	Odtwarzanie	R	R	R	R
3c	Powtarzanie próby	R	R	R	HR
4	Płynny upadek	R	R	HR	HR
5	Korekcja defektów metodami AI	–	NR	NR	NR
6	Rekonfiguracja dynamiczna	–	NR	NR	NR
7a	Metody strukturalne	HR	HR	HR	HR
7b	Metody półformalne (IEC 61131-3)	R	R	HR	HR
7c	Metody formalne	–	R	R	HR
8	CASE wspomagające specyfikację	R	R	HR	HR

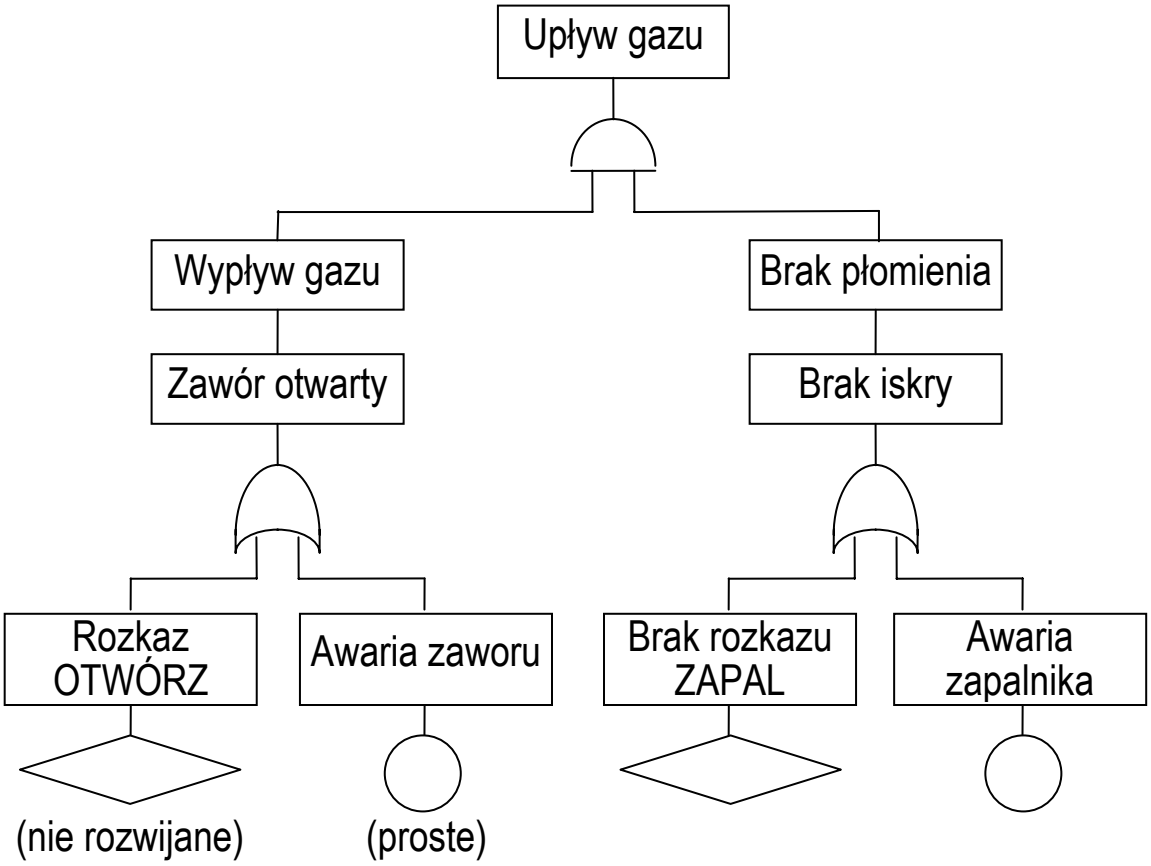
- Projektowanie szczegółowe i implementacja

	Technika/metoda	SIL1	SIL2	SIL3	SIL4
1a	Metody strukturalne	HR	HR	HR	HR
1b	Metody półformalne (IEC 61131-3)	R	R	HR	HR
1c	Metody formalne	–	R	R	HR
2	CASE wspomagające projektowanie	R	R	HR	HR
3	Podejście modułowe	HR	HR	HR	HR
4	Brak obiektów dynamicznych i skoków, ograniczenie przerwań, wskaźników i rekursji	R	HR	HR	HR
5	Programowanie strukturalne	HR	HR	HR	HR

Analiza bezpieczeństwa – metoda FTA

(PN-IEC 1025: Analiza drzewa niezdatności)

- Przykład: analiza palnika gazowego



Opis zdarzenia

- kod identyfikacyjny (wiąże z dokumentacją projektową)
- nazwa zdarzenia i opis
- prawdopodobieństwo, zależności czasowe, itp.

Metody analizy

- przegląd drzewa
- wyznaczenie funkcji boolowskich
- wyznaczenie minimalnych przekrojów (zbiorów zdarzeń powodujących wystąpienie zdarzenia szczytowego)

Schemat postępowania:

1. Analiza systemu i celów jego działania
2. Identyfikacja zdarzeń zagrażających.
3. Budowa drzewa niezdatności dla każdego zdarzenia.
4. Badanie drzewa w celu określenia:
   - zdarzeń prostych powodujących uszkodzenie systemu
   - oszacowanie tolerancji na uszkodzenia
   - prawdopodobieństwa uszkodzenia systemu
   - lokalizacji elementów krytycznych

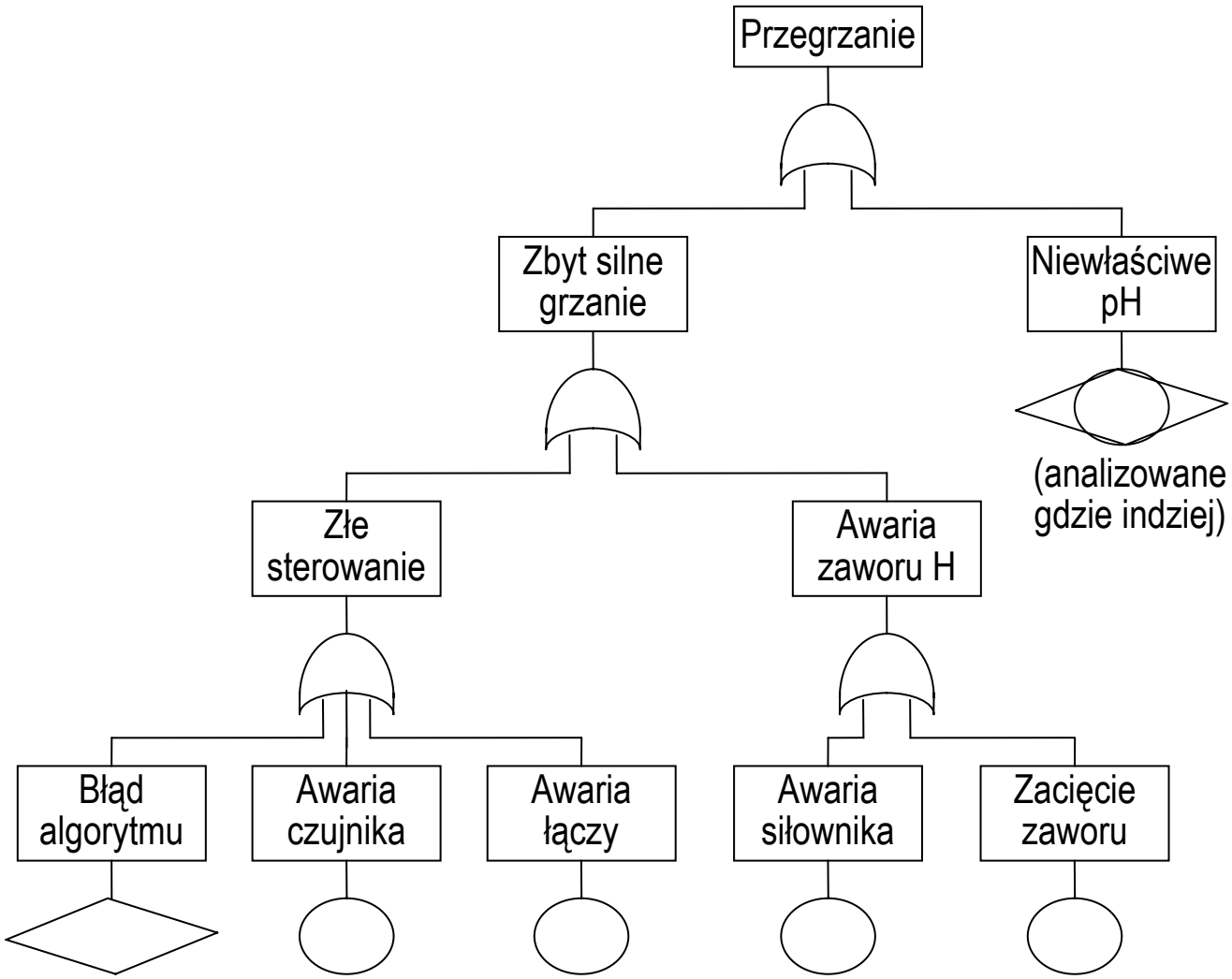
→ Podczas projektu:

- wprowadzenie zabezpieczeń (elementy, funkcje).
- określenie planu diagnostyki, spodziewanych napraw.

- Przykład: instalacja chemiczna

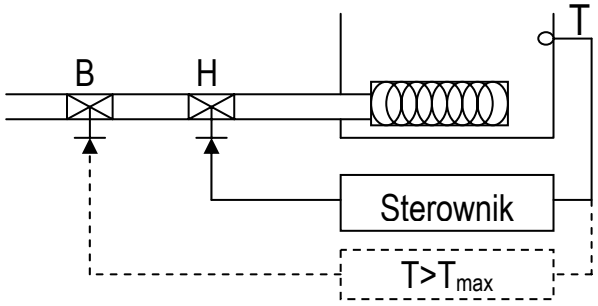
- reaktor (z dopływami składników)
- grzejnik reaktora z sterowanym zaworem H
- czujniki temperatury i pH
- sterownik z rozproszonym we/wy

Zdarzenie zagrażające: przegrzanie (grozi pożarem)



pojedyncze defekty prowadzą do zagrożenia!

→ Zawór zabezpieczający



Drzewo niezdatności