Servus,
hier einmal ein sehr detailliertes mathematisches Beispiel für einen Safety-Nachweis:

1 STS

Es sei ein Zustandstransitionssystem STS $=< S, S_0, Next >$ gegeben, mit:

$$\begin{aligned} S &= \{1,2,3,4,5\} \\ S_0 &= \{1\} \\ Next &= \{<1,2>,<2,3>,<3,4>,<4,2>,<4,5>\} \end{aligned}$$

2 Safety-Eigenschaft

$$\forall \sigma \in S^\infty : \ \sigma \notin \Pi \ \Rightarrow (\exists i \ \forall \zeta \in S^\infty : \ pre(\sigma, i) \circ \zeta \notin \Pi)$$

3 Eigenschaft 1

Nur am Anfang kann der Zustand 1 erreicht werden. Einmal verlassen darf er nicht wieder auftreten!

$$\Pi_1 = \{1\}^* \circ \{2,3,4,5\}^\infty$$

3.1 Beweis

$$\begin{aligned} \forall \sigma \in S^\infty \wedge \sigma \notin \Pi_1 &\Rightarrow \sigma \in \{1\}^* \circ \{2,3,4,5\}^* \circ \{1\} \circ S^\infty && (1) \\ (1) &\Rightarrow \exists i :< s_i, 1 > \text{ mit } s_i \neq 1 && (2) \\ (1) \wedge (2) &\Rightarrow pre(\sigma, i) \in \{1\}^* \circ \{2,3,4,5\}^* \circ \{1\} && (3) \\ (3) &\Rightarrow pre(\sigma, i) \circ \zeta \in \sigma \in \{1\}^* \circ \{2,3,4,5\}^* \circ \{1\} \circ S^\infty && (4) \\ (4) &\Rightarrow pre(\sigma, i) \circ \zeta \notin \Pi_1 && (5) \end{aligned}$$

3.2 Erklärung

1: Wenn $\sigma \notin \Pi_1$ ist, muss nach endlicher Zeit eine 1 auftauchen, obwohl vorher keine 1 stand!

2: Man wähle i genauso, dass man die erste Stelle auf die in (1) hingewiesen hat nimmt.

3: Folglich schneidet man dort σ ab

4: Hier wird nur beschrieben in welcher Menge $pre(\sigma, i) \circ \zeta$ liegt.

5: Diese Menge ist disjunkt von Π_1

4 Eigenschaft 2

Wie aus der Übung: Es gibt keine Transition von 1 zur 5:

$$\Pi_2 = \{\sigma \in S^\infty \mid \nexists i : s_i = 1 \wedge s_{i+1} = 5\}$$

4.1 Beweis

$$\begin{aligned}
\forall \sigma \in S^\infty \wedge \sigma \notin \Pi_2 &\Rightarrow \sigma \in S^* \circ \{1\} \circ \{5\} \circ S^\infty && (6)\\
(1) &\Rightarrow \exists i : s_i = 1 \wedge s_{i+1} = 5 && (7)\\
(1) \wedge (2) &\Rightarrow pre(\sigma, i) \in S^* \circ \{1\} \circ \{5\} && (8)\\
(3) &\Rightarrow pre(\sigma, i) \circ \zeta \in \sigma \in S^* \circ \{1\} \circ \{5\} \circ S^\infty && (9)\\
(4) &\Rightarrow pre(\sigma, i) \circ \zeta \notin \Pi_2 && (10)
\end{aligned}$$

4.2 Erklärung

Eigentlich genau das gleiche wie bei der ersten Eigenschaft