Intuition:

Gegeben sei ein Prozess Q und ein Property-Prozess P mit αP $\subseteq \alpha$Q. Sei w ein beliebiger Ablauf von Q. Durch die parallele Komposition von Q mit dem Property-Prozess P wird jede Aktion in w, die auch im Alphabet von P vorkommt, im LTS von P in eindeutiger Weise (da lts(P) deterministisch und vollständig) begleitet (durch Aktionssynchronisation). Erreicht man auf diese Weise den Fehlerzustand, dann ist $w|_{\alpha P}$ ein illegaler Ablauf (bzgl. P) und umgekehrt.

Satz 1:

Sei P ein Property-Prozess und Q ein (gewöhnlicher) FSP-Prozess mit αP $\subseteq \alpha$Q und $\pi \notin$ lts(Q). Q $\models$ P **genau dann**, **wenn** in lts(Q $\|$ P) der Fehlerzustand nicht erreichbar ist.

Automatisches Checken von Sicherheitseigenschaften:

Durch Breitensuche im LTS von (Q $\|$ P) nach Erreichbarkeit des Fehlerzustands kann entschieden werden, ob ein Prozess Q eine Sicherheitseigenschaft P erfüllt oder nicht.

Beweisskizze für Satz 1:

„⇒" Bew. durch Umkehrschluss.

Ann.: Sys $lts(Q \| P)$ ist π ermöglicht.

$\Rightarrow \exists\, w \in \propto(Q\|P)^* = \propto Q^*$ mit $(q_0, p_0) \xrightarrow{w}{}^{*}_{lts(P\|Q)} (q, \pi) = \pi$

($\propto(Q\|P)^* = \propto Q^*$ da $\propto P \subseteq \propto$; $q \neq \pi$, weil $\pi \notin lts(Q)$.)

Def. $lts(P\|Q)$

$\Downarrow$

$\Rightarrow$ (1) w ist endlicher Anfang eines Ablaufs w' von Q,

(2) $p_0 \xrightarrow{w|\propto P}{}^{*}_{lts(P)} \pi$

$\Rightarrow$ $w'|\propto P$ hat einen endlichen Anfang, nämlich $w|\propto P$, der im $lts(P)$ zu einem Fehlerzustand führt.

Def. $\Rightarrow$ $w'|\propto P$ ist keine legale Aktionenfolge bzgl. P

Def. $\vDash$ $\Rightarrow$ $Q \not\vDash P$.

$\Leftarrow$ " Beweis durch Widerspruch.

"

Ann: $Q \neq P$

Def. $\vdash$ $\Rightarrow$ $\exists$ Schluss w von Q, so dass $w|_{\alpha P}$ nicht legal ist bzgl. P

Def. "legal" $\Rightarrow$ $\exists$ endl. Aufzug $\underset{\downarrow}{w_P}$ von $w|_{\alpha P}$ mit $p_0 \xrightarrow[\mathrm{Hn}(P)]{w_P^*} \pi$ ($w_P^* \in \alpha P^*$)

$\Rightarrow$ $\exists$ endl. Aufzug $w_Q \in \alpha Q^*$ von w mit

$w_Q|_{\alpha P} = w_P$ und $(q_0, p_0) \xrightarrow[\mathrm{Hn}(P \| Q)]{w_Q^*} (q, \pi) = \pi$

$\Rightarrow$ der Fehlerzustand ist in $\mathrm{Hn}(Q \| P)$ erreichbar

□