Variáveis para o gerenciamento de Hazards

Funcionalidade: fnct / fnct'. Indica que a funcionalidade estava corretamente implementada (fnct) e continua (fnct')

Hazards: {(H, P)}, h / h'. "h" é o conjunto de Hazards e respespectivas probabilidades anteria "h" e ~~posteria~~ "h'". Cada Hazard é composto do elemento perigoso, passos para ativá-lo e o destino do Hazard.

O antes: versão anterior. O depois: feita a análise, deve ter:
- Hazards filhos
- Novos Hazards
- Hazards c/ novas probabilidade de ocorrer.

Versão inicial do sistema:

$h = \{ \top_H \} \Rightarrow$ É o topo dos hazards. Significa que nem todos os hazards foram encontrados. Var nova? pndn (pendente)

$fnct = false$

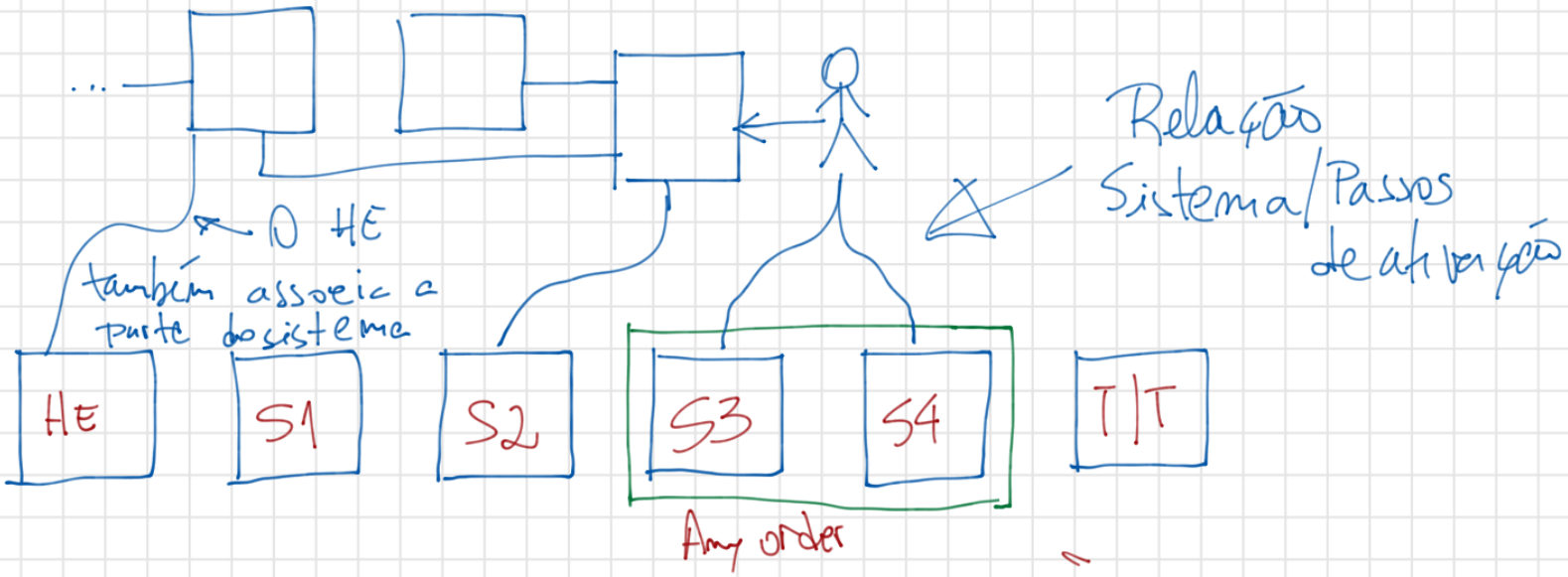
$h' = \{(H_1, \bot)\}$

$fnct' = true$

$\neg fnct \wedge fnct'$ (h don't care)

$fnct \wedge fnct' \wedge h' \preceq h \wedge \neg pndn \wedge \neg pndn'$

$(pndn \vee pndn') \wedge fnct \wedge fnct' \wedge h \preceq h' \Rightarrow$ podem ter aumentado os hazards.


...
HE
também associa a parte do sistema
HE
S1
S2
S3
S4
T|T
Any order
Relação Sistema/Passos de ativação