Bridge Controller: "Old" and "New" Events



Bridge Controller: Guards of "old" Events 2nd Refinement



Bridge Controller: Guards of "new" Events 2nd Refinement



PO/VC Rule of **Invariant Preservation**: Sequents





Discharging POs of m2: Invariant Preservation First Attempt

 $ML_out/inv2_4/INV$ $\frac{H \vdash P \quad H \vdash Q}{H \vdash P \land Q} \quad \text{AND}_R \quad \frac{H, P, Q \vdash R}{H, P \land Q \vdash R} \quad \text{AND}_L$ $\frac{H, P, Q \vdash R}{H, P, P \Rightarrow Q \vdash R} \quad \text{IMP}_L \quad \frac{H, P \vdash Q}{H \vdash P \Rightarrow Q} \quad \text{IMP}_R$



 $d \in \mathbb{N}$ d > 0

 $n \in \mathbb{N}$ $n \le d$ $a \in \mathbb{N}$ $b \in \mathbb{N}$

C E N

areen ≠ red

a+b+c=n

 $a = 0 \lor c = 0$ $ml_t \in COLOUR$ $il \ tl \in COLOUR$

 $ml_t = green$

COLOUR = { green, red }

 $ml_tl = green \Rightarrow a + b < d \land c = 0$ $il_tl = areen \Rightarrow b > 0 \land a = 0$

 $iI_t = green \Rightarrow b > 0 \land (a+1) = 0$



Discharging POs of m2: Invariant Preservation

First Attempt



Fixed

Understanding the Failed Proof on INV



Fixing m2: Adding an Invariant





