Modelling Environment

Brendan Mahony
Jim McCarthy
Kylie Williams

Trustworthy Systems

Defence Science and Technology Group

Formality

critical systems

- formal mathematical modelling and reasoning
- provide assurance: effective/adequate mitigations
- tool support

Compositionality

seamless (de)composition of systems

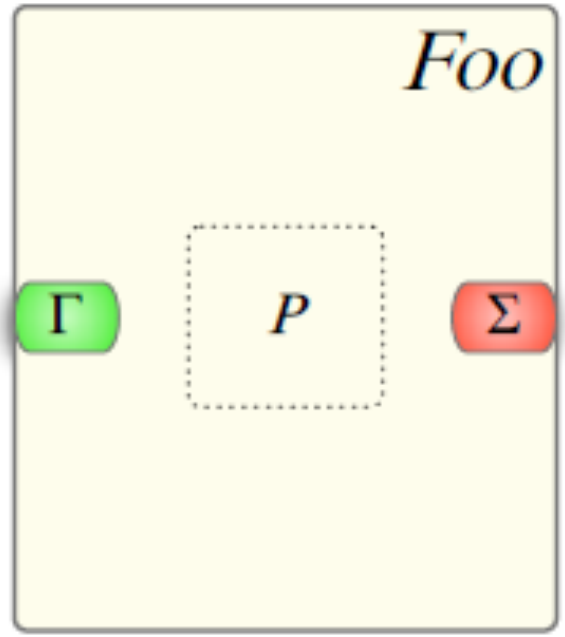
- understandable chunks for exposition
- “divide and conquer” localisation of reasoning
- coherent integration:
  - component hierarchy (design layers)
  - assurance hierarchy

Closed computation element

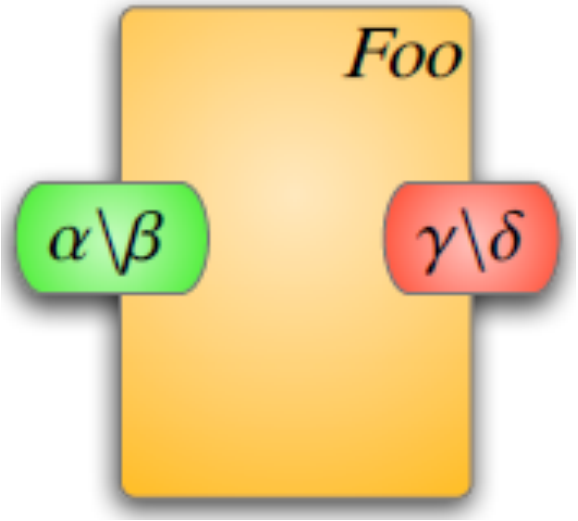
Signature:

is typing data; e.g.,

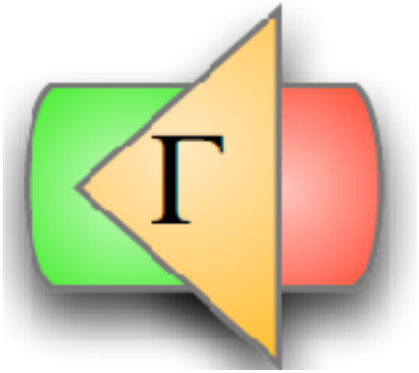
x:nat; …

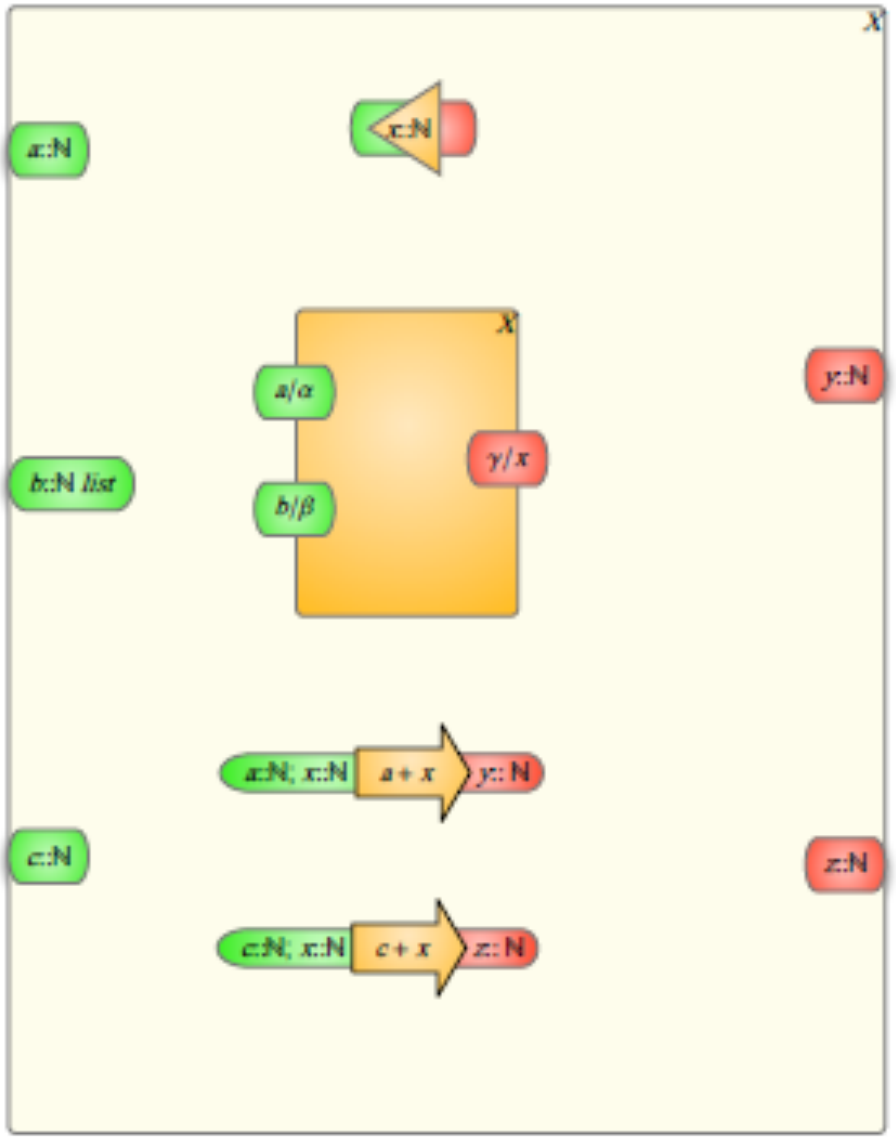


Open network

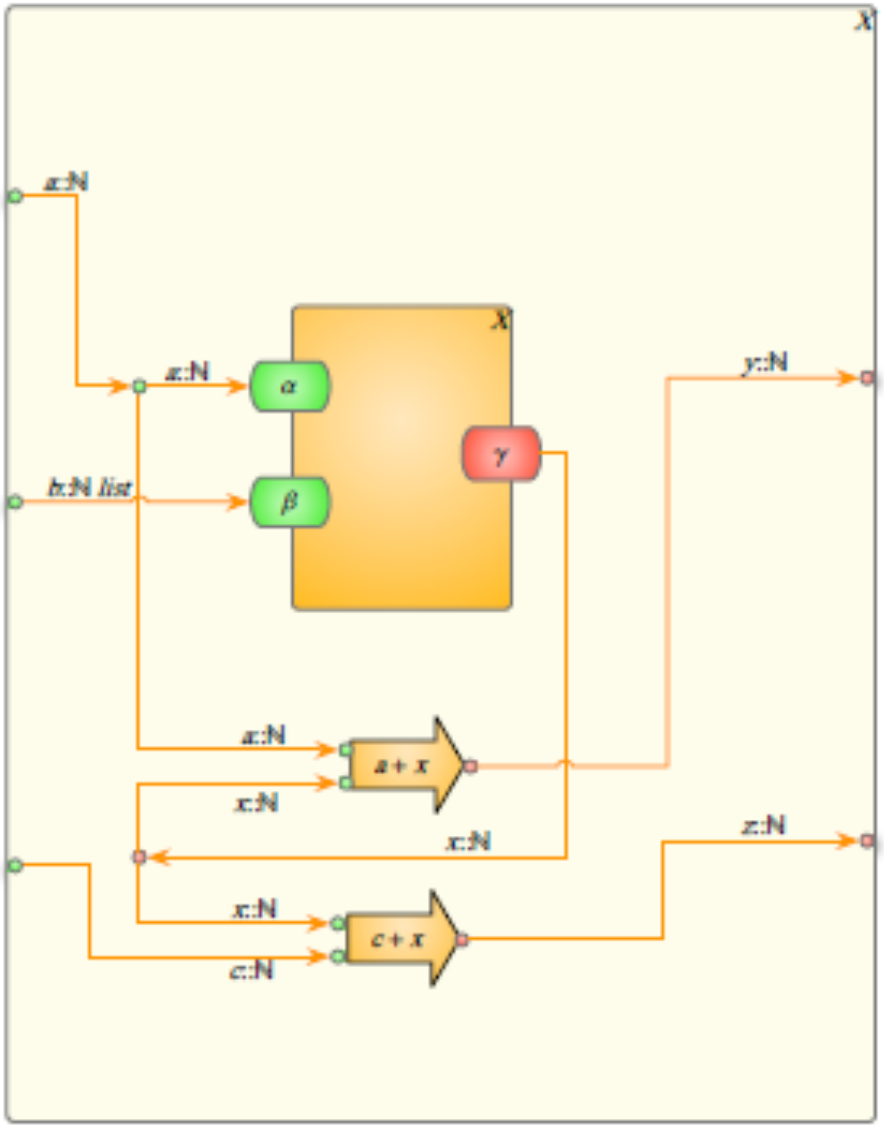


Feedback

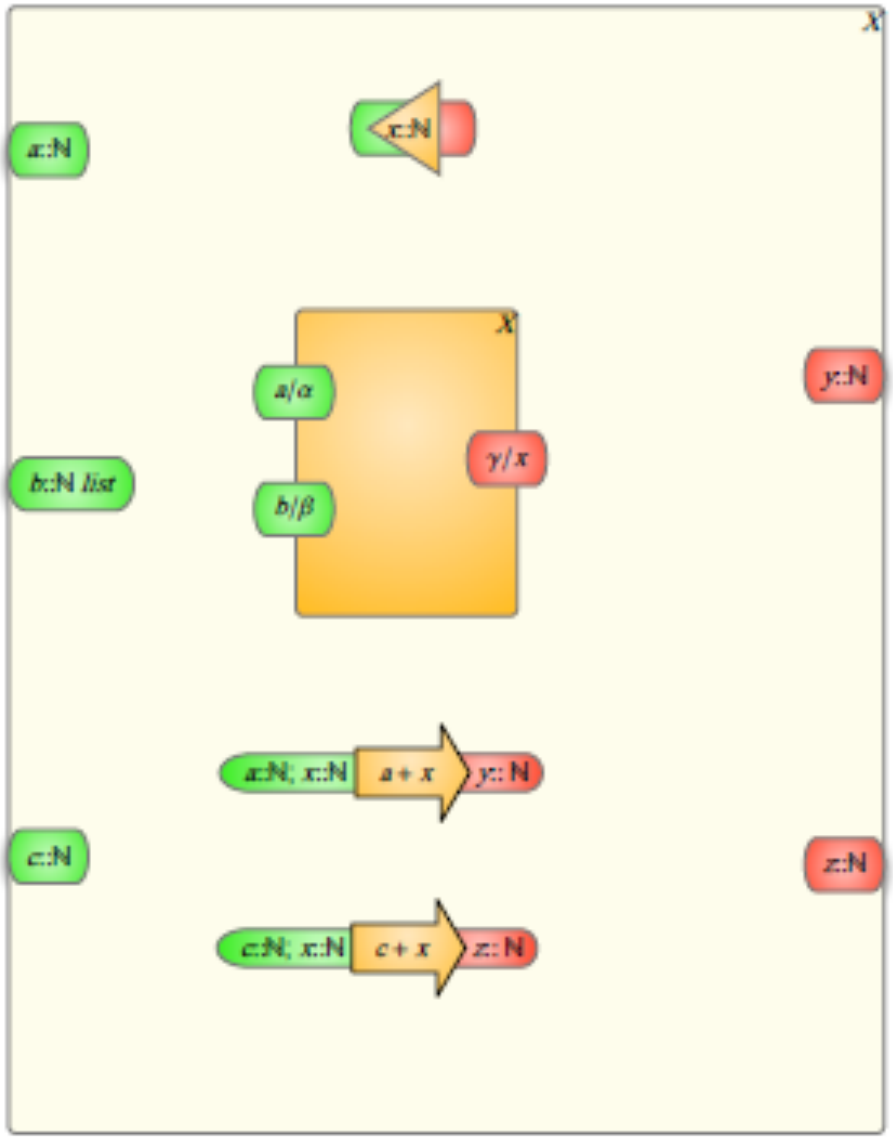




Tuple state bad



Record state good



Proof Assistant

algebras

- “signature algebra”

$$\Gamma : \Sigma \rightarrow \mathrm{TYPE}$$

- “state algebra” of records

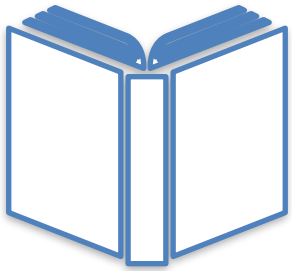
$$\sigma : (\forall\ n{:}\ \Sigma \bullet \Gamma\ n)$$

- “system algebra” of computations

Proof Assistant

idea!

- these algebras provide a computation paradigm
- suggests foundational logic based on records
- uniformity from theories through



?