Imperial College
London

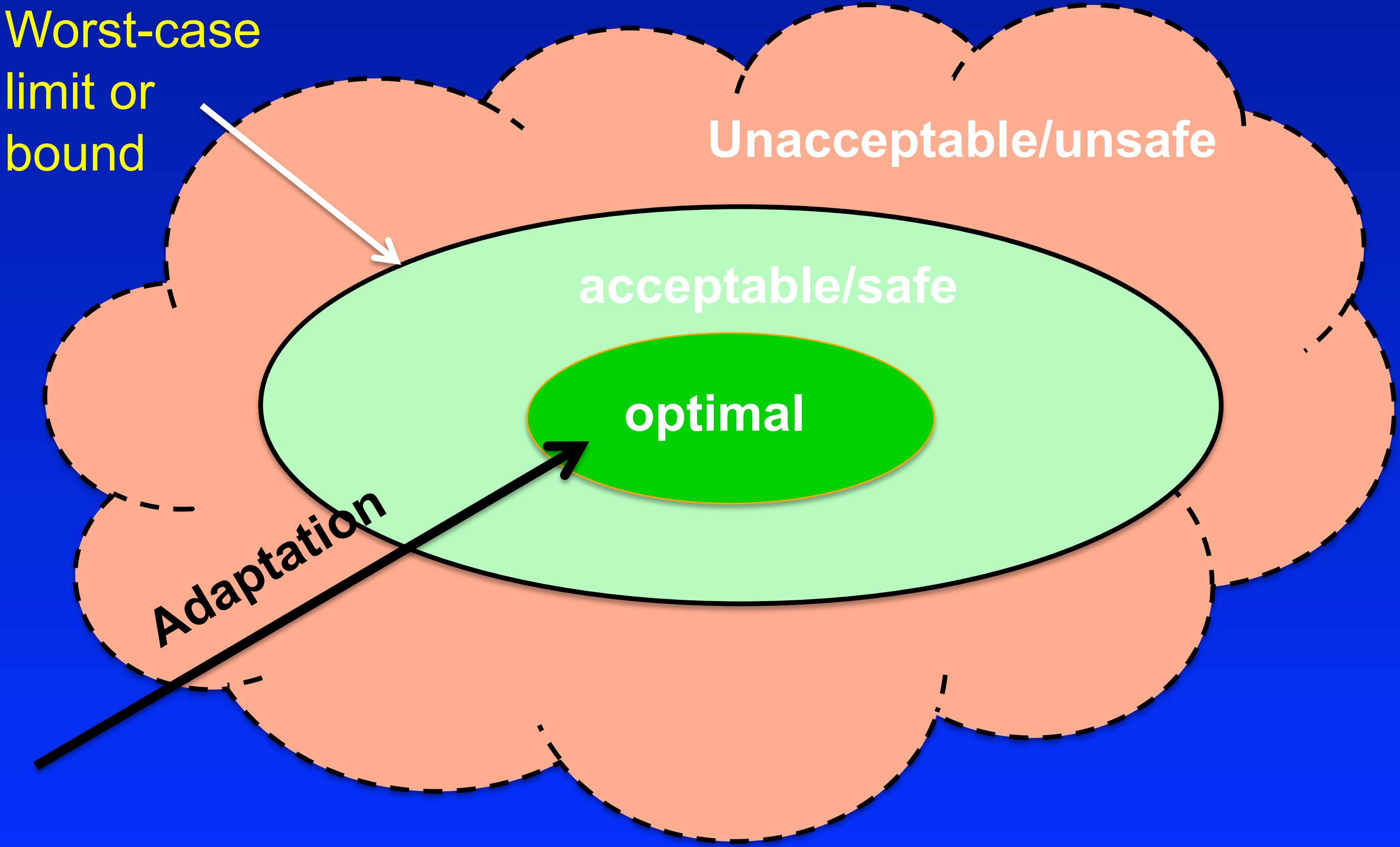
Assuring the Limits

in self-adaptable systems

Jeff Magee

SEAMS 2011

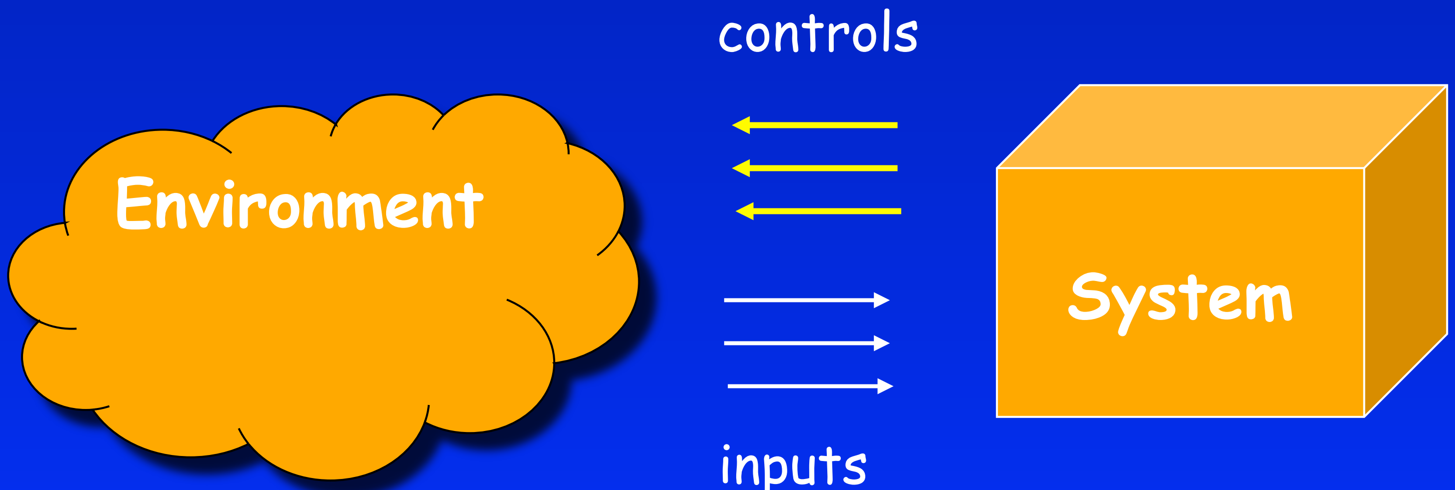
in general


Worst-case
limit or
bound
Unacceptable/unsafe
acceptable/safe
optimal
Adaptation

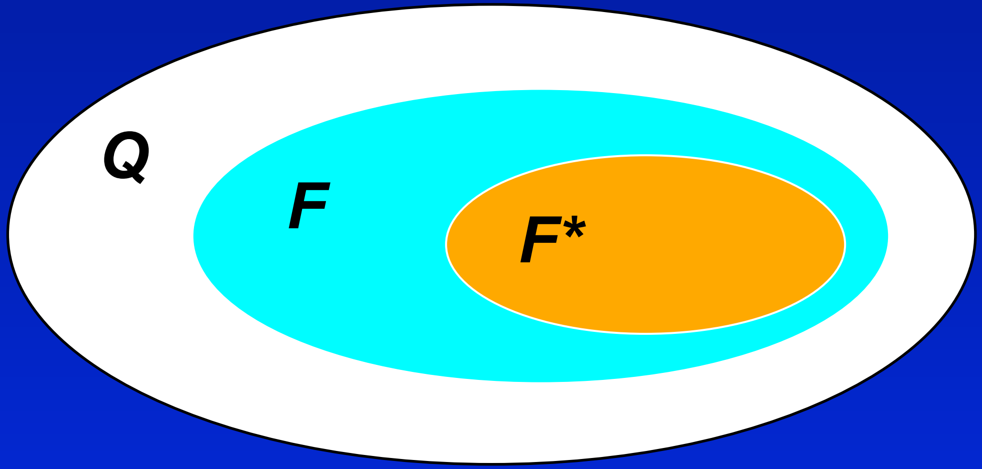
an example

Plan Synthesis

Consider plan as a winning strategy in an infinite two player game between the environment and the system such that goal **G** is always satisfied no matter what order of inputs from environment.



plan synthesis*



safety game

Q = set of states

F = set of accepting states (G holds)

F* = set of winning states found iteratively such that transition out of ***F**** is via a controlled action.

* *Symbolic Controller Synthesis*.., Asarin, Maler, Pneuli, 1989

liveness

$$\left(\bigwedge_{i=1}^{k}\Box S_i\right)\wedge\left(\bigwedge_{j=1}^{m}\Box\Diamond J_j^2\rightarrow\bigwedge_{l=1}^{n}\Box\Diamond J_l^1\right)$$

No Safety Violations!

Using Safety Game algorithm

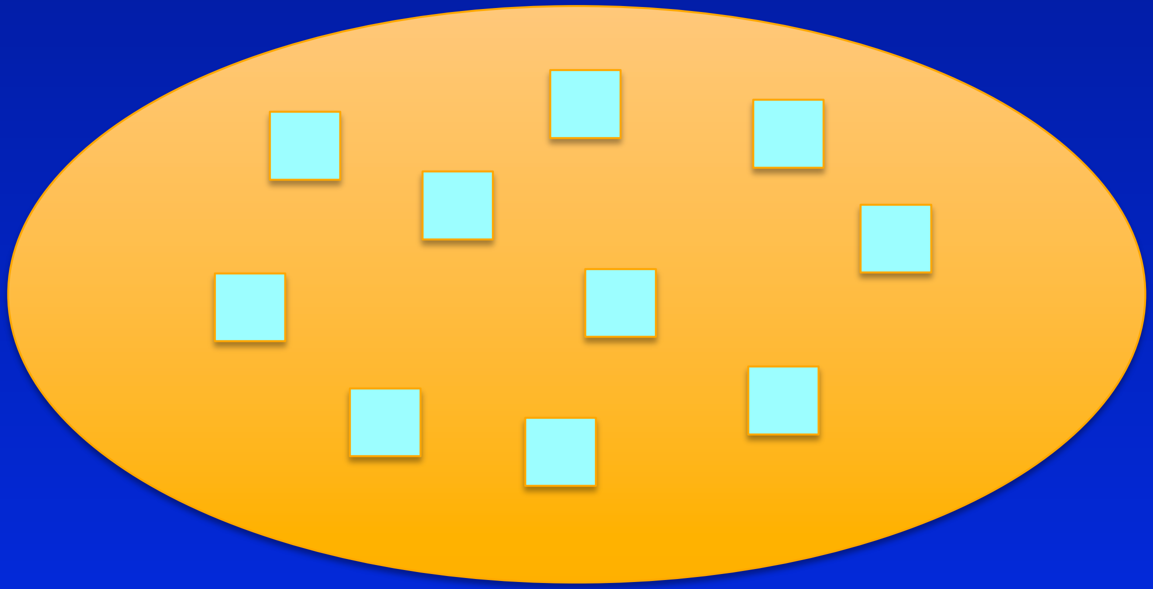
$$\left(\bigwedge_{j=1}^{m}\Box\Diamond J_j^2\rightarrow\bigwedge_{l=1}^{n}\Box\Diamond J_l^1\right)$$

Liveness Assumptions

Liveness Guarantees

See "*Synthesis of Live Behaviour Models for Fallible Domains* ", ICSE 2011

decentralised co-ordination



Guaranteed bounds on global utility function*

* Alex Rogers, Alessandro Farinelli, Ruben Stranders, Nicholas R. Jennings: Bounded approximate decentralised coordination via the max-sum algorithm. Artif. Intell. 175(2): 730-759 (2011)

the engineering challenge

- “limits” cannot be an emergent property of self-adaptive systems

– must be engineered in a way so that worst-case limits are assured

– *by construction?*