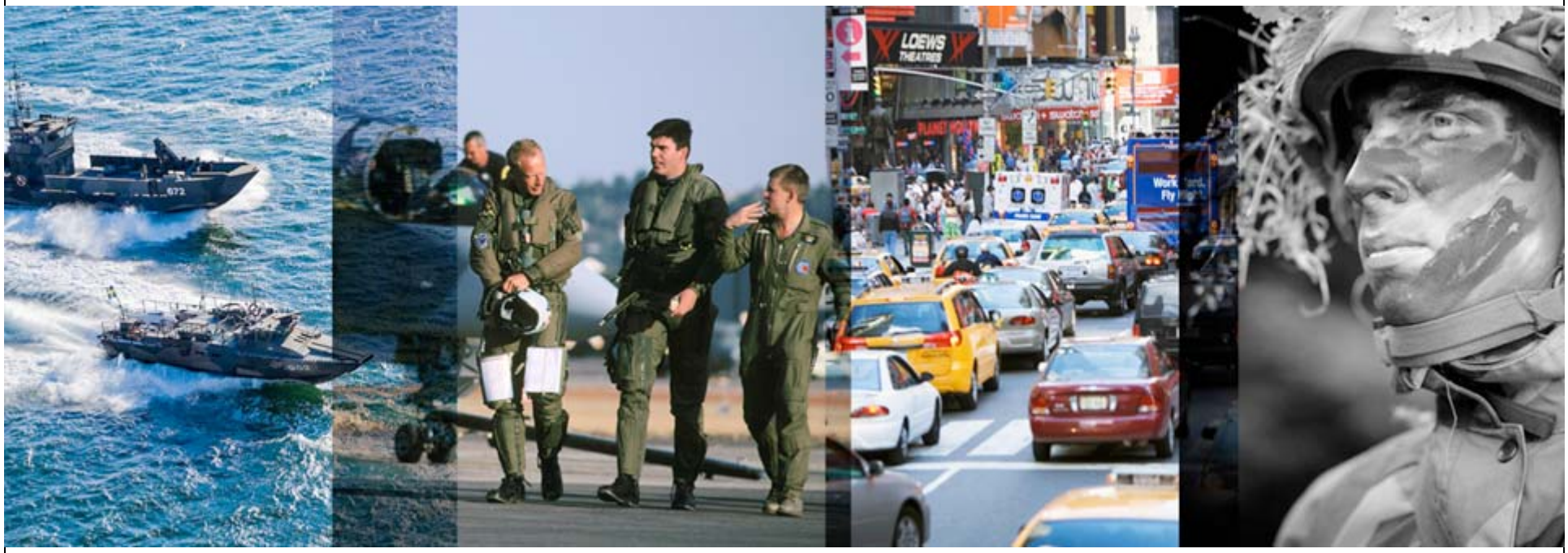
# Contracts based specification

## Results from the SPEEDS project




**Erik Herzog,** Ph.D.

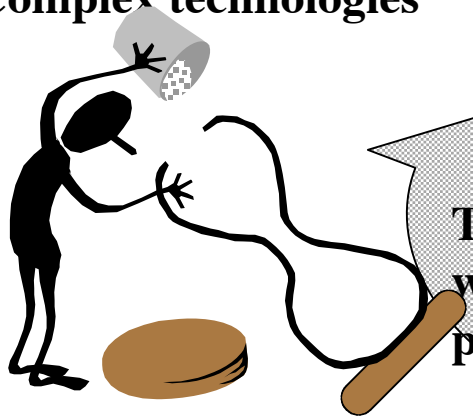
**2008-11-19**

**Sesam**

# Life - It would be trivial if it wasn't for

Complex technologies

Integrated into complex products



Things will be even worse for the next product generation

Change is constant

Developed in complex organisations

# Will things get better with models?

- Modelling allow for exposition of interfaces
- Improved clarity
- But traditional modelling languages does not make a distinction between what is required and what is assumed in terms of interface statics and dynamics

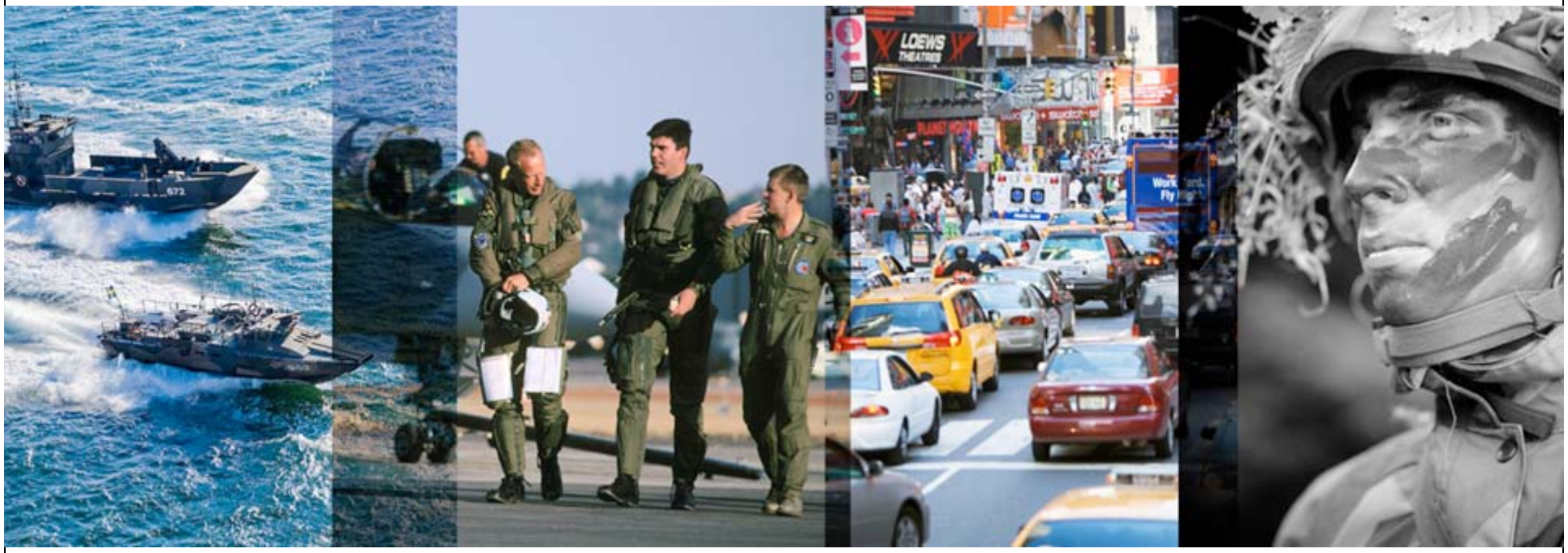
# The challenge

- Concurrent engineering
  - How to document and manage uncertainty
- Efficient coordination between cooperating teams
- Early virtual integration of components
  - Integrate models

# Systems Engineering Strategy

- To master complexity we abstract,
- Partition into components
- Integrate
- Problems
  - We do not know the details when we partition
  - Component development is difficult to coordinate
  - Things never work the first time we integrate

# Improving modelling practise



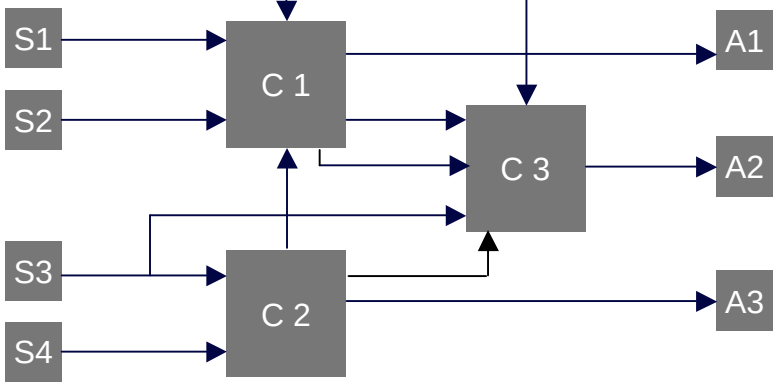
# What about the formal methods

- Formal methods has over and over again demonstrated their strength on small problems
- Any complex system will by nature be costly to formalise
  - Especially considering verification
- Limitations on what can be proven
- For system specification, where the model is an abstraction of the real system, any proof is just valid on that abstraction level
  - Weak connection to the real system

# Initially...

Design was king





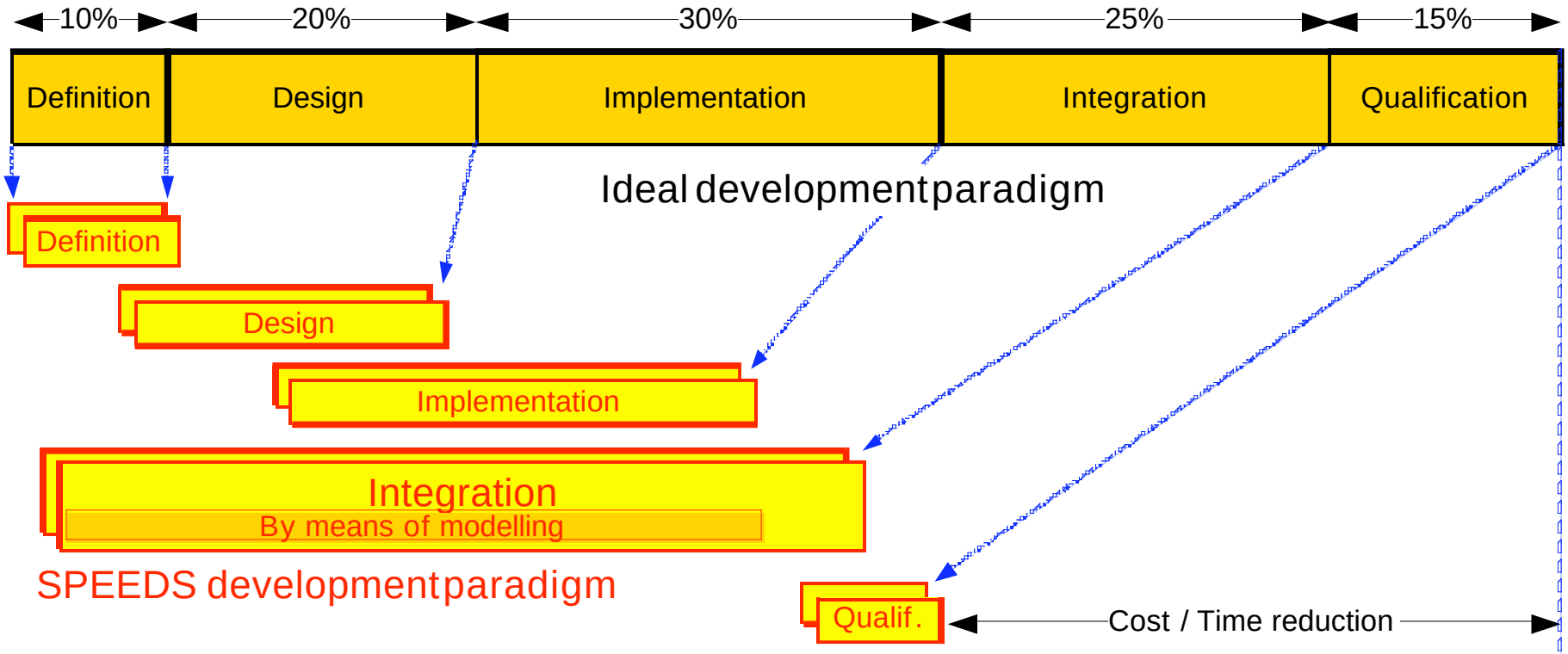

Focus on requirements

One-way communication

Raise Assumptions to the same dignity as requiremetns

Explicit capture of assumptions is important

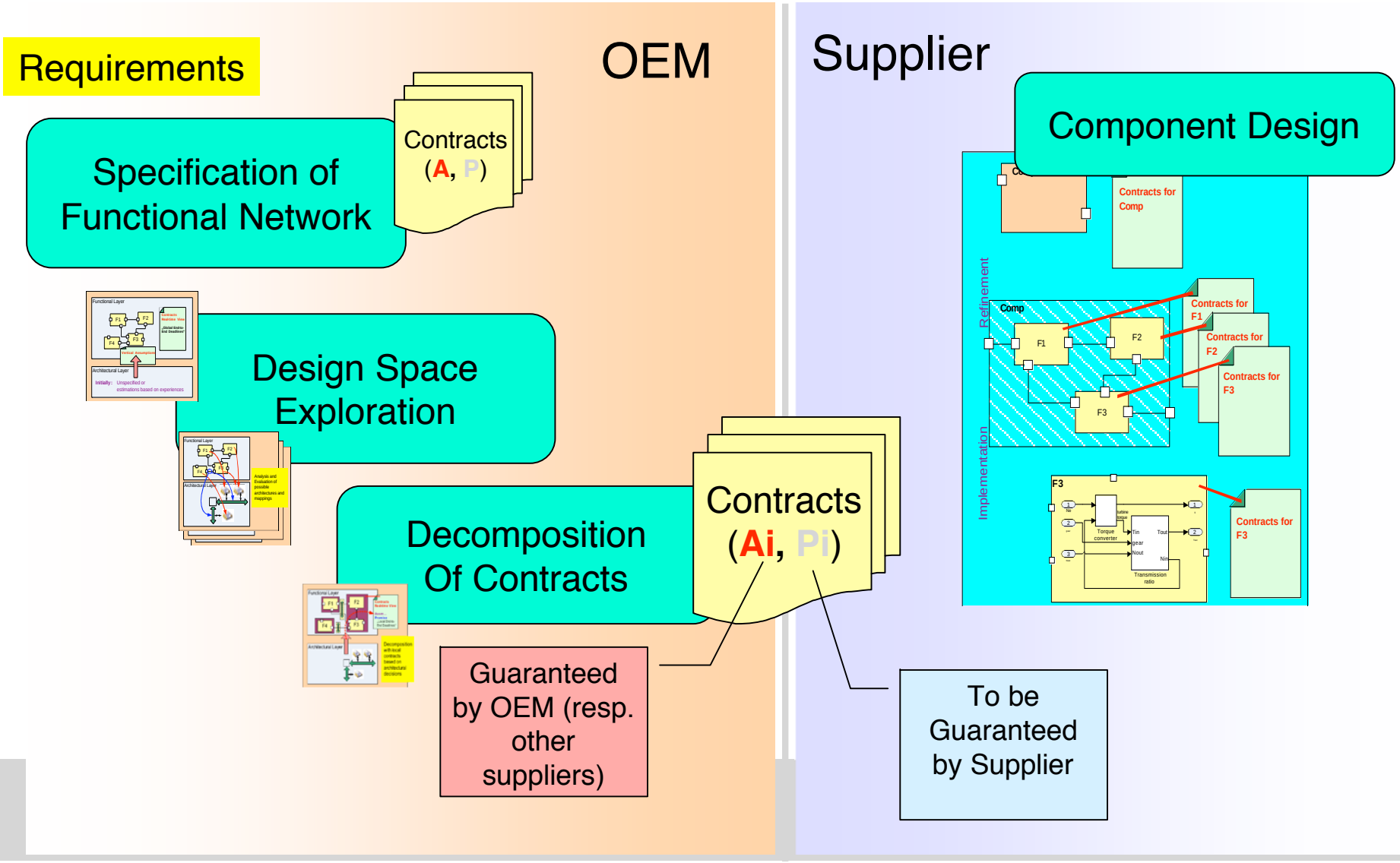
# What do we want to achieve?



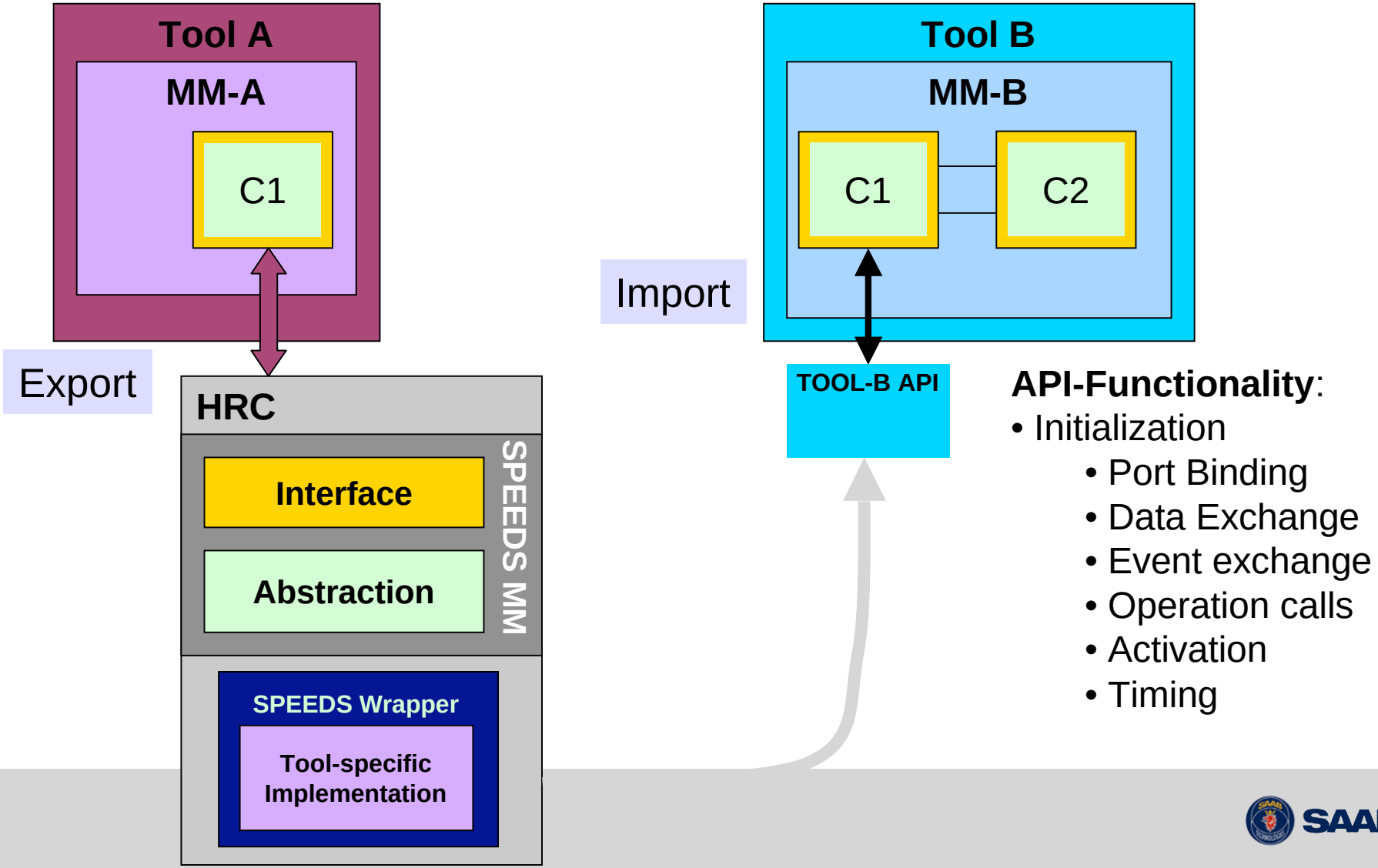
# SPEEDS

- MBSE requires a new approach to really take off
- Focusing of formality, interfaces and requirements
- Define
  - The Component (Component Based Engineering)
  - Requirements (Promises) on the component
  - Prerequisites  (Assumptions) on the environement for requirement fulfillment
  - Group *Assumptions* and *Promises* to *Contracts*
  - Formalise *Assumptions* and *Promises* where desirable
- Integrate
  - Synchronise C*ontracts* to discover integration problems
- Simulate
  - Hosted simulation
- Verify
  - Applying formal analysis

# Contracts in the design process



# Hosted simulation

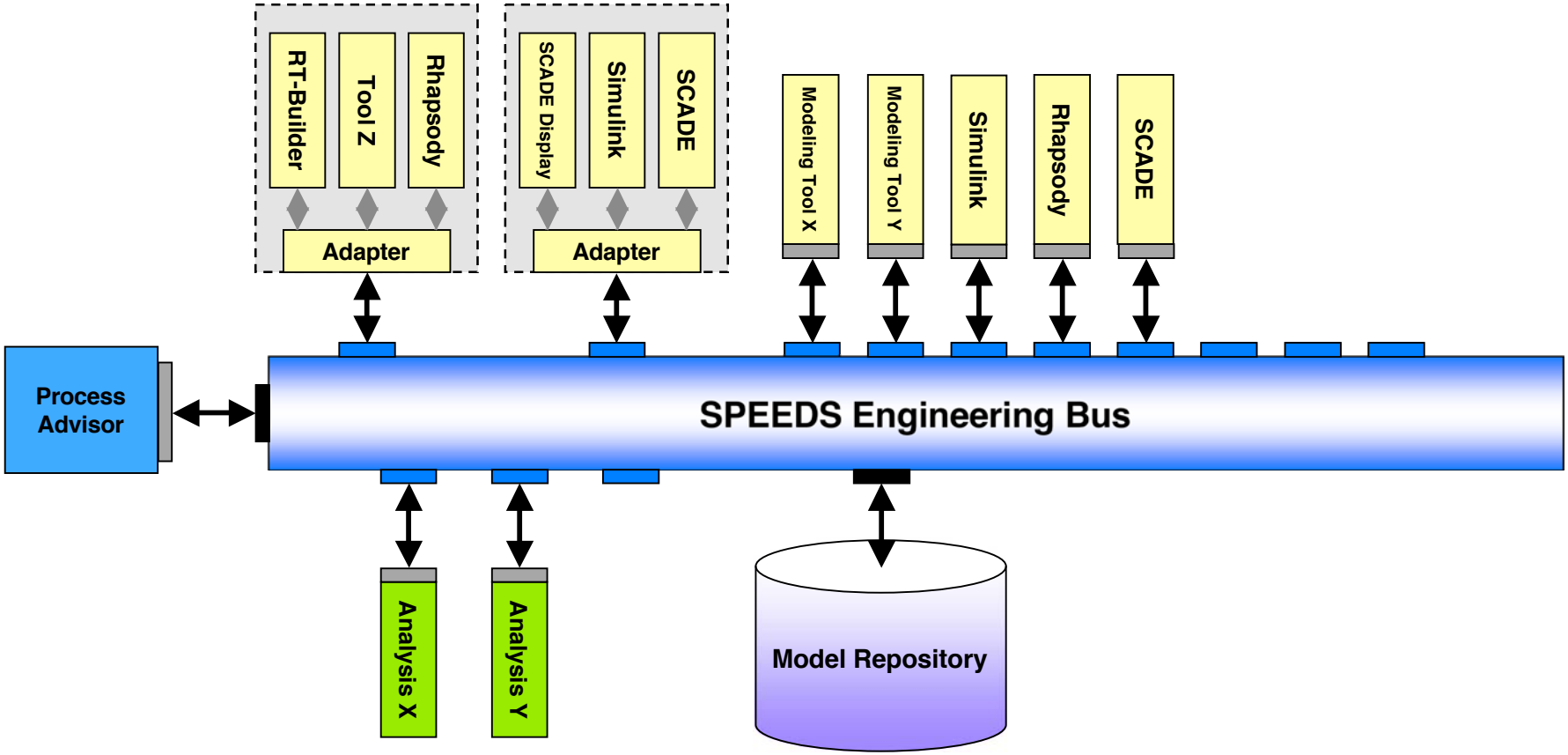



**API-Functionality**:

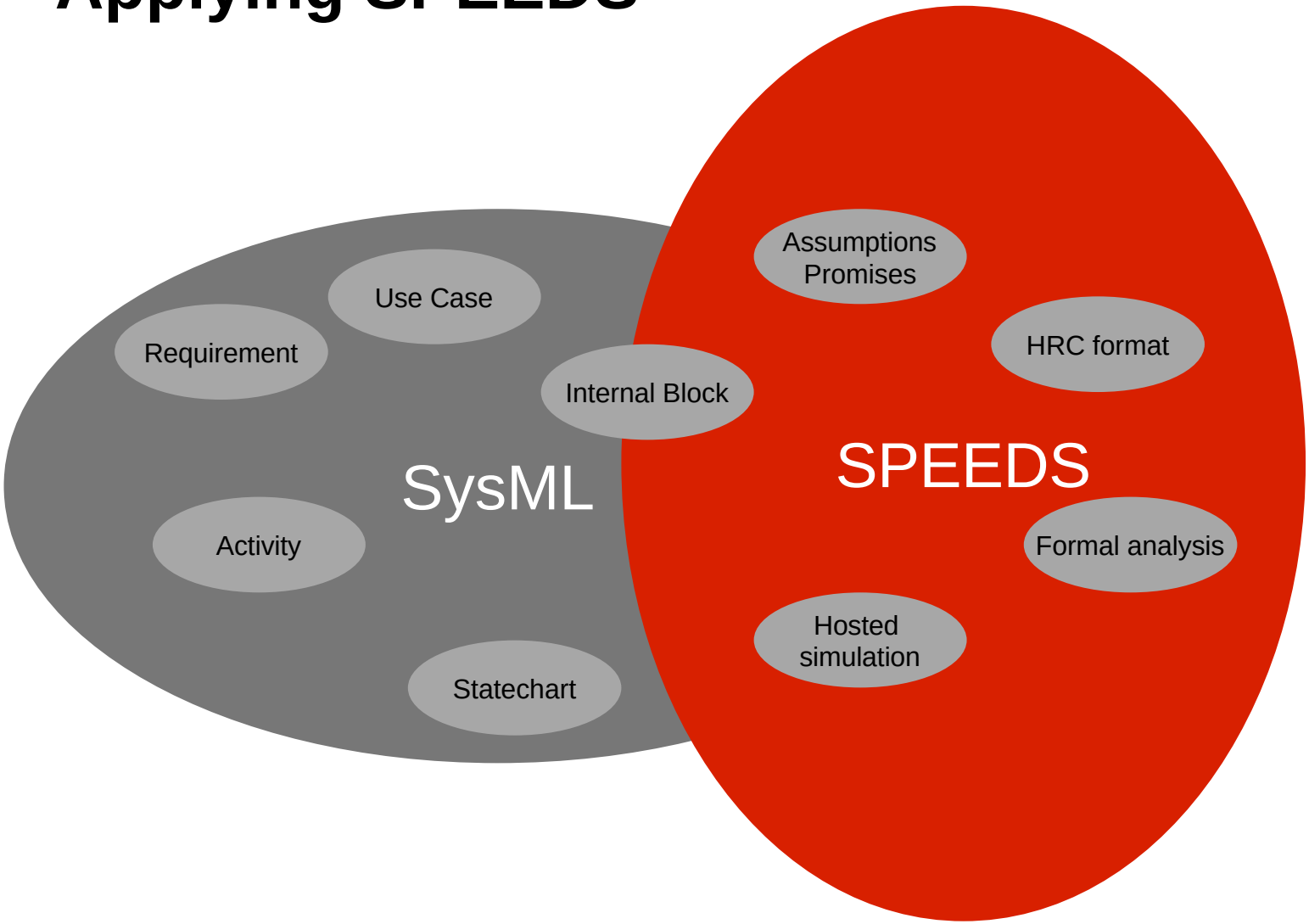
- Initialization
  - Port Binding
  - Data Exchange
  - Event exchange
  - Operation calls
  - Activation
  - Timing

SAAB

# Tool integration



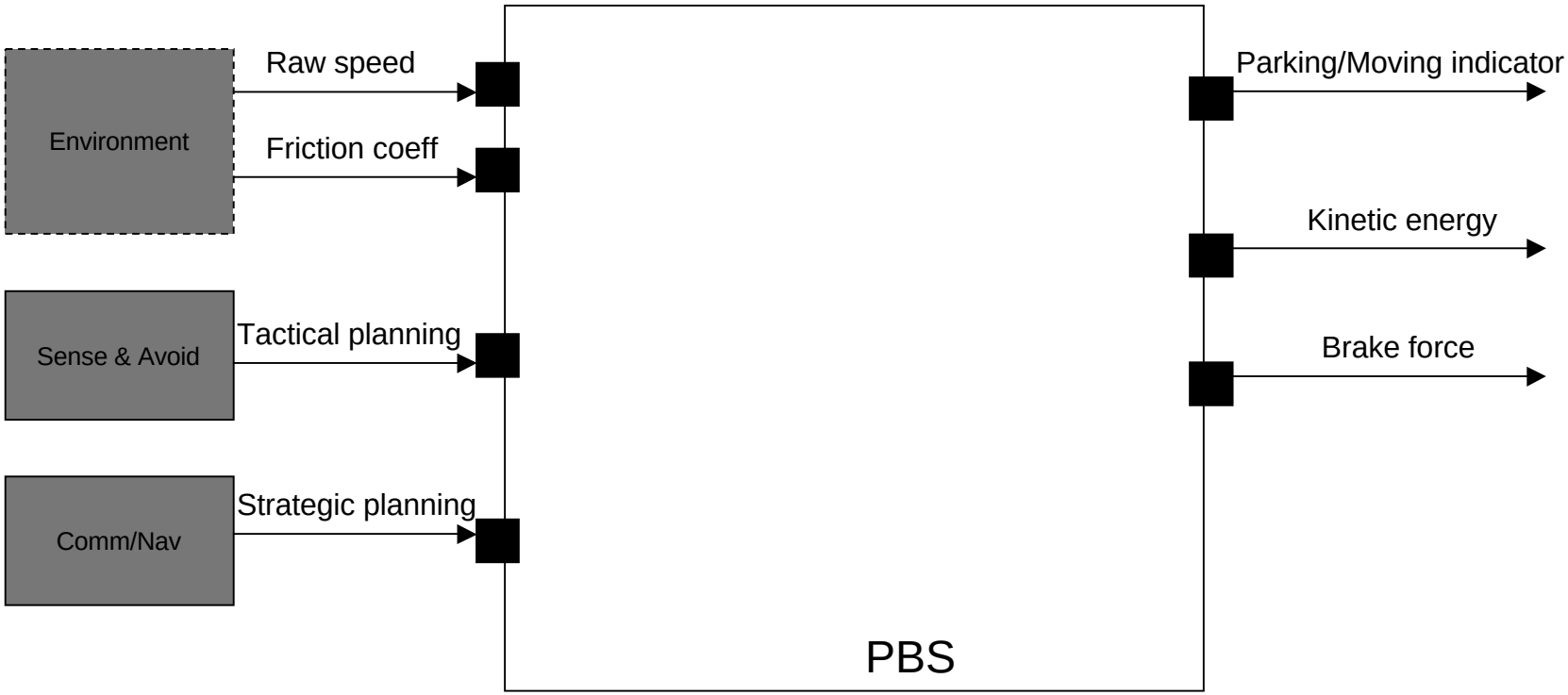
# Applying SPEEDS



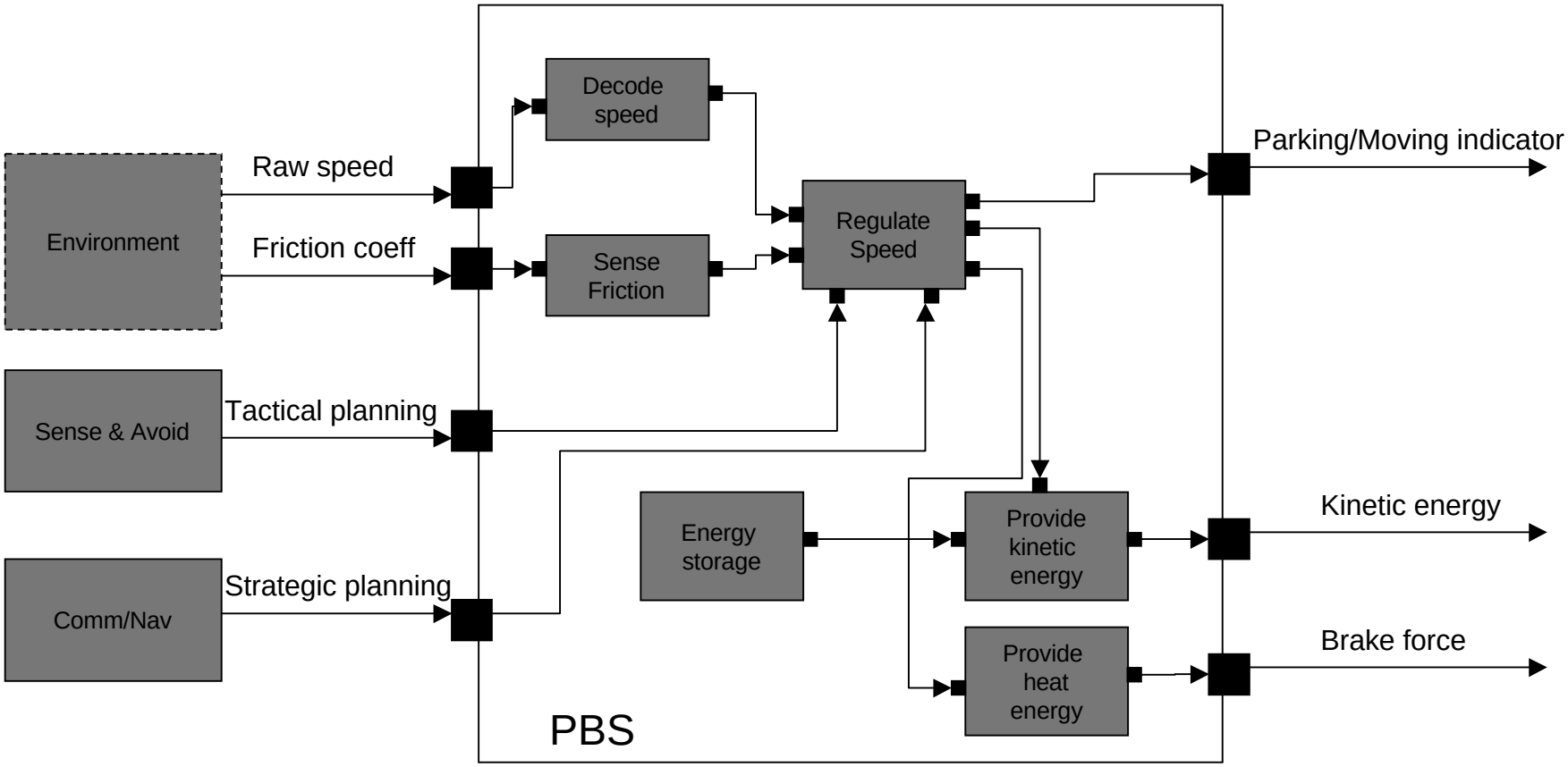
# Approach

- Use standard SysML tool as front-end
  - Telelogic Rhapsody
- Apply normal SysML modelling process
  - Views
  - Use cases
  - Activity diagrams
- Capture system functional (or physical) components and their interfaces
  - Using SysML Internal Block Diagrams used
- Identify requirements (promises) and constraints for individual interfaces
  - Using specific Assumption/Promise editor

# External Interfaces



# Internal functionality



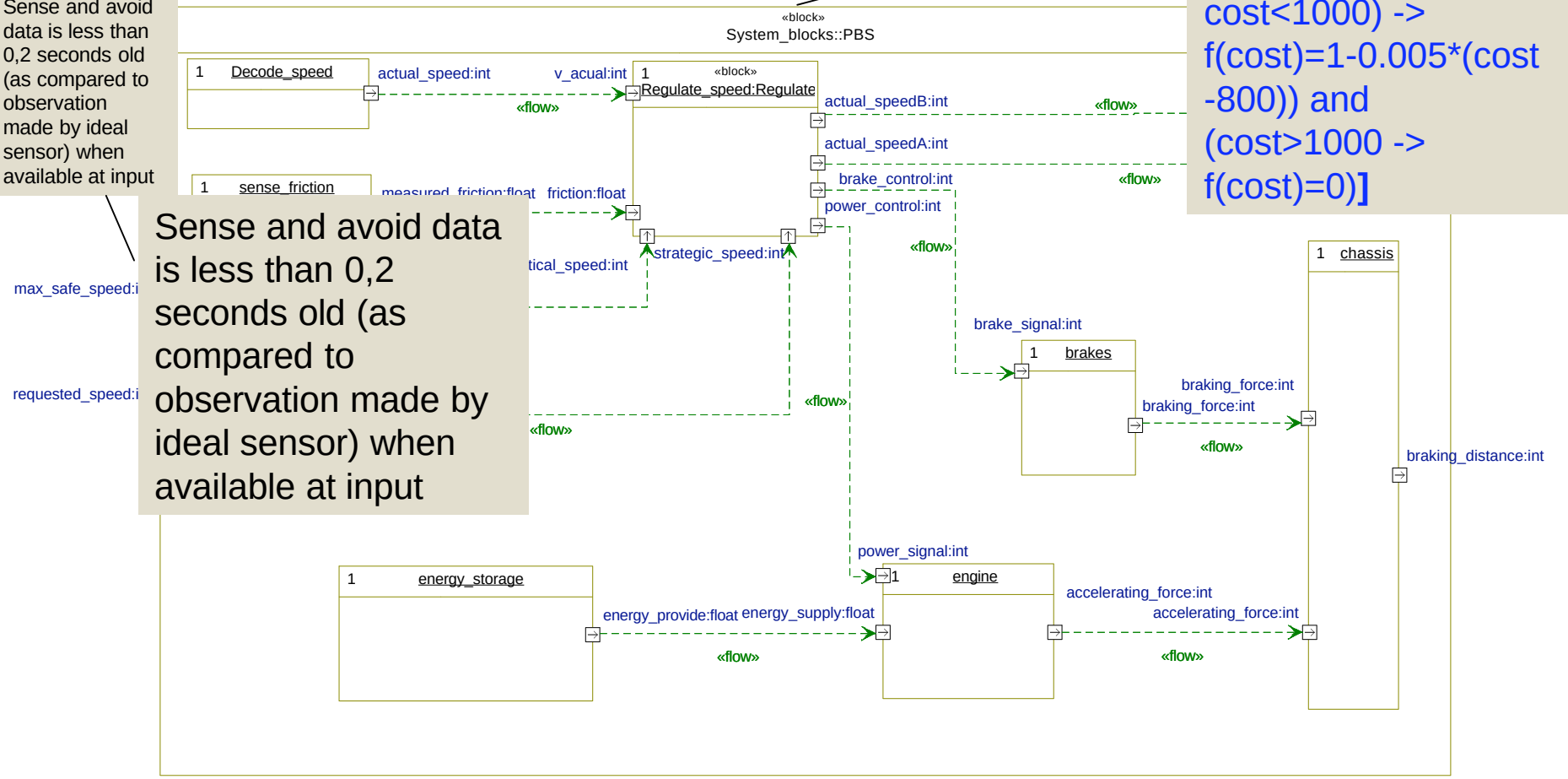
# Assumptions and Promises in u

PBS total cost is less than €1000, specifically:
f(c
f(c
f(c

**Always[**(cost<800 -> f(cost)=1) and ((cost>=800 and cost<1000) -> f(cost)=1-0.005*(cost -800)) and (cost>1000 -> f(cost)=0)**]**

Sense and avoid data is less than 0,2 seconds old (as compared to observation made by ideal sensor) when available at input

Sense and avoid data is less than 0,2 seconds old (as compared to observation made by ideal sensor) when available at input



# Experience from early validation

- Strengths
  - Promises couples to functionality or properties that a component is capable of controlling
  - Assumptions is a natural way to capture the constraints identified
    - Seldom done today
    - Prerequisite for concurrent engineering and comprehensive review
  - Coupling of assumptions and promises first step in the integration process
- Weaknesses
  - All assumptions and promises are captured on ports
    - Not natural for component properties
- Observations
  - Time consuming to formalise contracts
  - Extra effort for applying formal analysis may not be economical


SAAB

# SAABGROUP.COM