Modeling Cyber-Physical Systems

Towards a Holistic Integrated Approach

Manfred Broy

Technische Universität München
Institut für Informatik
D-80290 Munich, Germany
When modeling CPS we have capture following aspects:

- interaction – exchange of information/material
- distribution – structuring systems in architectures with elements related to locations
- context – operational system’s environment
- real time
- probability
- physicality
- …

To do that we have to use concepts

- interfaces – scope and interaction
- state – state transition
- architecture – (de-)composition
Basic System Modeling Concepts
System and its context
Basic System Notion: What is a discrete system (model)

A system has

• a system boundary that determines
  ◊ what is part of the systems and
  ◊ what lies outside (called its context)

• an interface (determined by the system boundary), which determines,
  ◊ what ways of interaction (actions) between the system und its context are possible (static or syntactic interface)
  ◊ which behavior the system shows from view of the context (interface behavior, dynamic interface, interaction view)

• a structure and distribution addressing internal structure, given
  ◊ by its structuring in sub-systems (sub-system architecture)
  ◊ by its states und state transitions (state view, state machines)

• quality profile

• the views use a data model

• the views may be documented by adequate models
Discrete systems: the modeling theory

Sets of typed channels

\[ I = \{ x_1 : T_1, x_2 : T_2, \ldots \} \]
\[ O = \{ y_1 : T'_1, y_2 : T'_2, \ldots \} \]

syntactic interface

\[ (I \triangleright O) \]

data stream of type \( T \)

\[ \text{STREAM}[T] = \{ \text{IN}\backslash\{O\} \rightarrow T^* \} \]

valuation of channel set \( C \)

\[ \text{IH}[C] = \{ C \rightarrow \text{STREAM}[T] \} \]

interface behaviour for syn. interface \( (I \triangleright O) \)

\[ [I \triangleright O] = \{ \text{IH}[I] \rightarrow \emptyset (\text{IH}[O]) \} \]

interface specification

\[ p: I \cup O \rightarrow IB \]

represented as interface assertion \( S \)

logical formula with channel names as variables for streams

Towards a uniform model: Basic system model

**System class**: distributed, reactive systems

System consists of
- named components (with local state)
- named channels

**Driven by a global, discrete clock**
Timed Streams: Semantic Model for Black-Box-Behavior

Message set:
\[ M = \{a, b, c, \ldots\} \]

Messages transmitted at time \( t \)

Infinite channel history

\[ \langle a, d, a, b \rangle \]
Modeling Interface Behavior
The Basic Behaviour Model: Timed Streams and Channels

\[ C \] set of channels

Type: \[ C \rightarrow \text{TYPE} \] type assignment

\[ x : C \rightarrow (\mathbb{N}\setminus\{0\} \rightarrow M^*) \] channel history for messages of type \( M \)

\( \bar{C} \) or \( \text{IH}[C] \) set of channel histories for channels in \( C \)
System interface model

Channel: Identifier of Type stream

I = \{ x_1 : D_1, x_2 : D_2, ... \} set of typed input channels
O = \{ y_1 : T_1, y_2 : T_2, ... \} set of typed output channels

Syntactic interface: \( (I \triangleright O) \)

Interface behavior

\( F : \vec{I} \rightarrow \wp(\vec{O}) \)

Set of interface behaviours with input channels I and output channels O:

\( \text{IF}[I \triangleright O] \)

Set of all interface behaviours:

\( \text{IF} \)
(I ⊳ O)  syntactic interface with set of
input channels I and of output channels O

F : \( \bar{I} \rightarrow \wp(\bar{O}) \)  semantic interface for (I ⊳ O)
with timing property addressing strong causality
(let \( x, z \in \bar{I}, y \in \bar{O}, t \in \mathbb{IN} \)):

\[
x \downarrow t = z \downarrow t \Rightarrow \{y \downarrow t+1 : y \in F(x)\} = \{y \downarrow t+1 : y \in F(z)\}
\]

\(x \downarrow t\)  prefix of history \(x\) of length \(t\)

A system shows a total behavior
Continuous systems: the model

Sets of typed channels

\[ I = \{x_1 : T_1, x_2 : T_2, \ldots \} \]
\[ O = \{y_1 : T'_1, y_2 : T'_2, \ldots \} \]

syntactic interface

\((I \triangleright O)\)

continuous data stream of continuous type \( M \)

\[ \text{ConSTREAM}[T] = \{\mathbb{IR}_+ \rightarrow M\} \]

valuation of channel set \( C \)

\[ \text{CIH}[C] = \{C \rightarrow \text{ConSTREAM}[T]\} \]

interface behaviour for syn. interface \((I \triangleright O)\)

\[ [I \triangleright O] = \{\text{CIH}[I] \rightarrow \emptyset(\text{CIH}[O])\} \]

interface specification

\[ p : I \cup O \rightarrow IB \]

represented as interface assertion \( S \)

logical formula with channel names as variables for continuous streams

Discrete systems: the modeling theory - probability

Sets of typed channels

\[ I = \{ x_1 : T_1, x_2 : T_2, \ldots \} \]
\[ O = \{ y_1 : T'_1, y_2 : T'_2, \ldots \} \]

syntactic interface

\[ (I \rightarrow O) \]

data stream of type \( T \)

\[ \text{STREAM}[T] = \{ \text{IN}\backslash\{0\} \rightarrow T^* \} \]

valuation of channel set \( C \)

\[ \text{IH}[C] = \{ C \rightarrow \text{STREAM}[T] \} \]

interface behaviour for syn. interface \((I \rightarrow O)\)

\[ [I \rightarrow O] = \{ \text{IH}[I] \rightarrow \text{PD}[\varnothing (\text{IH}[O])] \} \]

interface specification

\[ p : I \cup O \rightarrow \text{IB} \]

represented as interface assertion \( S \)

logical formula with channel names as variables for streams

Extensions of the model

• Physical Aspects & Properties: Rich Models
  ◊ Space
  ◊ Geometry
  ◊ Temperature
  ◊ …

Evolution and Development: Specification, Refinement, Compatibility
Interface Specification

• An interface model describes in a particular abstraction the interface behavior of a system
  ◊ interface behavior for syn. interface \((I \triangleright O)\)
  \([I \triangleright O] = \{IH[I] \rightarrow \wp(IH[O])\}\)
  ◊ interface specification by a predicate
    \(p : I \cup O \rightarrow IB\)

written by an interface assertion

Example: System interface specification

A transmission component TMC

- **Spec name**
- **Input channel**
  - in $x: T$
  - out $y: T$
  - $x \sim y$
- **Output channel**

$x \sim y \equiv (\forall m \in T: \{m\} \circ x = \{m\} \circ y)$

Verification: Proving properties about specified components

From the interface assertions we can prove

• Safety properties

\[
\{m\}#y > 0 \land y \in TMC(x) \Rightarrow \{m\}#x > 0
\]

• Liveness properties

\[
\{m\}#x > 0 \land y \in TMC(x) \Rightarrow \{m\}#y > 0
\]
Structure:
Composition and Decomposition
Composing Interfaces

• Composition is an operation on syntactically compatible system interfaces

\[ \bigotimes : [I_1 \| O_1] \times [I_2 \| O_2] \rightarrow [I \| O] \]

• The operation \( \bigotimes \) induces a composition operation on specifications

Modularity: Rules of compositions for interface specs

\[ F_1 \otimes F_2 \]

\[ \exists z_{12}, z_{21} : S_1 \land S_2 \]

\[ \begin{array}{l}
\text{F1} \\
\text{in } x_1, z_{21}: T \\
\text{out } y_1, z_{12}: T \\
\text{S1} \\
\end{array} \]

\[ \begin{array}{l}
\text{F2} \\
\text{in } x_2, z_{12}: T \\
\text{out } y_2, z_{21}: T \\
\text{S2} \\
\end{array} \]
Refining Interfaces
Refinement

• The idea of system refinement is that systems are developed
  ◊ by a sequence of development steps
  ◊ each step produces a more refined system description
  ◊ there is a refinement relation between the current system description and the
    produced system description

• The refinement relation
  ◊ is a relation between systems descriptions

• The relation can be used as an idealized relationship between
  ◊ specifications to formalize the steps of gathering requirements in requirements
    engineering
  ◊ specifications and architectures to formalize the steps in design of going from
    requirements to architecture
  ◊ system specifications and implementations (e.g. by state machines)
  ◊ levels of abstraction
Refinement

- Given systems/specifications $S$ and $S'$ we write $S$ is_refined_to $S'$ (and also $S \approx \Rightarrow S'$) to express that $S'$ is a refinement of $S$.

- **Horizontal Refinement**: Property Refinement
  - Adding properties to a specification – reducing the non-determinism of a system description

- **Vertical Refinement**: Interaction granularity refinement
  - Changing the granularity of the interaction
  - Interesting case: Refinements between continuous and discrete models

Remark: Both refinement notions can be applied not only to interface models but to all kinds of models

Horizontal Refinement

\[ \tilde{F} : \tilde{I} \rightarrow \wp(\tilde{O}) \]

is refined by a behavior \( \hat{F} : \tilde{I} \rightarrow \wp(\tilde{O}) \)

if

\[ \forall x \in \tilde{I} : \hat{F}.x \subseteq F.x \]

we write

\[ F \approx_{IF} \hat{F} \]

Compositionality of refinement: Modularity

\[ \forall k : F_k \approx_{IF} \hat{F}_k \]

\[ \bigotimes\{F_k : k \in \mathbb{I}K\} \approx_{IF} \bigotimes\{\hat{F}_k : k \in \mathbb{I}K\} \]
Verification of refinement steps

• A system $F$ with behaviour assertion $Q$ is refined by a system $F'$ with behaviour assertion $Q'$ if and only if
  $$Q \iff Q'$$
  In other words: $F'$ is a refinement of $F$ if all properties of $F$ are also properties of $F'$
• The implication $Q \iff Q'$ shows also how to verify the refinement relation
Vertical refinement: Levels of abstraction

Theorems

- Property refinement implies interaction refinement
- Compositionality of interaction refinement
- Interaction refinement distributes over composition
- Abstractions of interaction refinements of implementations are interaction refinements of abstractions
- Time abstraction is interaction abstraction
- Interaction abstraction is a Galois connection
Compatibility

- A system $S'$ is called (replacement) compatible for system $S$ if $S'$ can be used instead of $S'$ in every system $M$ without violating the correctness of the system $M$
- **Compatibility** coincides with refinement in case of modular refinement
A flexible model of time

- Time is a key issue in embedded systems:
- Dealing with timing properties
  - Specification
  - Analysis
  - Verification
    - Analysis
    - Testing
    - Model checking
    - Deduction based verification
- Transforming time
- Dedicated models of time
  - Micro/Macro Step
  - Perfect synchrony
  - Scheduling
- Abstractions
Example: TMC with Timing Restrictions

TMC

\[
\begin{align*}
\text{in} & \quad x: T \\
\text{out} & \quad y: T \\
\forall t \in \mathbb{N}: \forall m \in T: \\
\{m\} \circ (x \downarrow t) & \geq \{m\} \circ (y \downarrow t+\text{delay}) \\
\{m\} \circ (x \downarrow t) & \leq \{m\} \circ (y \downarrow t+\text{delay}+\text{deadline})
\end{align*}
\]
Conclusion Refinement

- Refinement formalises development steps
- Going from
  - an interface specification to an architecture (design step)
  - an interface specification to a state machine (implementation)
  can be understood as special steps of refinement
- Compatibility is defined by refinement, too
- The change of time granularity is a refinement
Implementation: Systems as State Machines

The State View
System and States

• Systems have states
• A state is an element of a state space
• We characterize state spaces by
  ◊ a set of state attributes together with their types
• The behaviour of a system with states can be described by its state transitions
State model for systems/components

A system can be implemented by a state Machine

\( \Sigma \) set of states, initial state \( \sigma \subseteq \Sigma \)

State transition function:

\[ \Delta: (\Sigma \times (I \rightarrow M^*)) \rightarrow \mathcal{P} (\Sigma \times (O \rightarrow M^*)) \]

State transition diagram:

State Machines in general

A state machine \((\Delta, \Lambda)\) consists of

- a set \(\Sigma\) of states - the state space
- a set \(\Lambda \subseteq \Sigma\) of initial states
- a state transition function or relation \(\Delta\)
  
  - in case of a state machine with input/output:
    events (inputs \(E\)) trigger the transitions and events (outputs \(A\)) are produced by them respectively:
    \[\Delta : \Sigma \times E \rightarrow \Sigma \times A\]
  
  - in the case of nondeterministic machines:
    \[\Delta : \Sigma \times E \rightarrow \wp(\Sigma \times A)\]

- Given a syntactic interface with sets \(I\) and \(O\) of input and output channels:
  
  - \(E = I \rightarrow M^*\)
  
  - \(A = O \rightarrow M^*\)
A state machine \((\Delta, \Lambda)\) defines for each initial state
\[\sigma_0 \in \Lambda\]
and each sequence of inputs
\[e_1, e_2, e_3, \ldots \in E\]
a sequence of states
\[\sigma_1, \sigma_2, \sigma_3, \ldots \in \Sigma\]
and a sequence of outputs
\[a_1, a_2, a_3, \ldots \in A\]
through
\[(\sigma_{i+1}, a_{i+1}) \in \Delta(\sigma_i, e_{i+1})\]
In this manner we obtain computations of the form

\[
\sigma_0 \xrightarrow{a_1/b_1} \sigma_1 \xrightarrow{a_2/b_2} \sigma_2 \xrightarrow{a_3/b_3} \sigma_3 \quad \ldots
\]

For each initial state \(\sigma_0 \in \Sigma\) we define a function

\[
F_{\sigma_0} : \overline{I} \rightarrow \wp(\overline{O})
\]

with

\[
F_{\sigma_0}(x) = \{y : \exists \sigma_i : \sigma_0 = \sigma_0 \land \forall i \in \mathbb{IN}: (\sigma_{i+1}, y_{i+1}) = \Delta(\sigma_i, x_{i+1})\}
\]

\(F_{\sigma_0}\) denotes the interface behavior of the transition function \(\Delta\) for the initial state \(\sigma_0\).

Furthermore we define

\[
\text{Abs}(\langle \Delta, \Lambda \rangle) = F_{\Lambda}
\]

where:

\[
F_{\Lambda}(x) = \{y \in F_{\sigma}(x) : y \in F_{\sigma}(x) \land \sigma \in \Lambda\}
\]

\(F_{\Lambda}\) is called the interface behavior of the state machine \(\langle \Delta, \Lambda \rangle\).
Moore Machines

• A Mealy machine \((\Delta, \Lambda)\) with
  
  \[
  \Delta : \Sigma \times E \rightarrow \wp (\Sigma \times \Lambda)
  \]

  is called Moore machine if for all states \(\sigma \in \Sigma\) and inputs \(e \in E\) the set
  
  \[
  \text{out}(\sigma, e) = \{ a \in A : (\sigma, a) = \Delta(\sigma, e) \}
  \]

  does not depend on the input \(e\) but only on state \(\sigma\).

• Formally: then for all \(e, e' \in E\) we have
  
  \[
  \text{out}(\sigma, e) = \text{out}(\sigma, e')
  \]

Theorem: If is \((\Delta, \Lambda)\) a Moore machine the \(F_\Lambda\) is strong causal.
Interface Abstraction for State Machines

• For a given state machine with input and output we define the interface through
  ◊ its syntactical interface (signature)
  ◊ its interface behavior

• We call the transition of the state machine to its interface the interface abstraction.

Verification/derivation of interface assertions for state machines
• similar to program verification (find an invariant)
• needs sophisticated techniques
Observable Equivalence

• Two systems modelled by state machines
  \((\Delta_1, \Lambda_1)\) and \((\Delta_2, \Lambda_2)\)
  are observably equivalent iff they fulfil the equation

  \[
  \text{Abs}(\Delta_1, \Lambda_1) = \text{Abs}(\Delta_2, \Lambda_2)
  \]
Composition of the two state machines

Consider Moore machines $M_k = (\Delta_k, \Lambda_k)$ ($k = 1, 2$):

$\Delta_k: \Sigma_k \times (I_k \rightarrow M^*) \rightarrow \wp(\Sigma_k \times (O_k \rightarrow M^*))$

We define the composed state machine

$\Delta: \Sigma \times (I \rightarrow M^*) \rightarrow \wp(\Sigma \times (O \rightarrow M^*))$

as follows

$\Sigma = \Sigma_1 \times \Sigma_2$

for $x \in I$ and $(s_1, s_2) \in \Sigma$ we define:

$\Delta((s_1, s_2), x) = \{(s_1', s_2'), z|O) : x = z|I \land \forall k: (s_k', z|O_k) \in \Delta_k(s_k, z|I_k)\}$

This definition is based on the fact that we consider Moore machines.

We write

$\Delta = \Delta_1 \parallel \Delta_2$

$M = M_1 \parallel M_2 = (\Delta_1 \parallel \Delta_2, \Lambda_1 \times \Lambda_2)$
An example of an essential property ...

Interface abstraction distributes for state machines over composition

\[ \text{Abs}(\Delta_1, \sigma_1) \parallel (\Delta_2, \sigma_2) = \text{Abs}(\Delta_1, \sigma_1) \otimes \text{Abs}(\Delta_2, \sigma_2) \]
Conclusion Systems as State Machines

• Each state machine defines an interface behaviour
• Each interface behaviour represents a state machine
• State machines can be described
  ◊ mathematically by their state transition function
  ◊ graphically by state machine diagrams
  ◊ structured by state transition tables
  ◊ by programs
• State machines define a kind of operational semantics
• Systems given by state machines can be simulated
• From state machines we can generate code
  ◊ state machines can represent implementations
• From state machines we can generate test cases
Functional View: Functional Decomposition
Combining Functions

Given two functions $F_1$ and $F_2$ in isolation

We want to combine them into a function $F_1 \otimes F_2$
Combining Functions

Their isolated combination

\[ F_1 \otimes F_2 \]

\[ F_1 \]

\[ F_2 \]

\[ I_1 \]

\[ I_2 \]

\[ O_1 \]

\[ O_2 \]
Combining Functions

If services $F_1$ and $F_2$ have feature interaction we get:

We explain the functional combination $F_1 \otimes F_2$ as a refinement step.
The steps of function combination

Given the isolated function $F_1$

We construct a refinement $F'_1$

And combine $F'_1$ with a refinement $F'_2$ of $F_2$

Functional architecture: functional decomposition

• The system interface behaviour \( F \) as specified by the system requirements specification \( A = \{A_i: 1 \leq i \leq n\} \) is structured
  
  ◇ into a set of sub-interfaces for sub-functions \( F_1, \ldots, F_k \)
  
  ◇ that are specified independently by introducing a number of mode channels to capture their feature interactions
  
  ◇ each \( F_i \) sub-function is described by
    
    • a syntactic interface and
    
    • an interface assertion \( B_i \) such that
      
      \[ \land \{B_i: 1 \leq i \leq k\} \Rightarrow A \]
Function Hierarchy

F₁, . . . , n

B₁ → B₂ → ... → Bₙ

F₁,₂

B₁ → B₂

F₁

B₁

F₂

B₂

... 

Fₖ

Bₖ

... 

Bₖ

Fₖ₊₁

Bₖ₊₁

Bₖ

... 

Bₙ

Fₙ

Bₙ

← sub subservice relation

channels of mode types
Model Integration
Integrating modeling concepts

• An architecture can be abstracted into an interface behavior
  ◊ Proof techniques for architecture verification

• A state machine can be abstracted into an interface behavior
  ◊ Proof techniques for implementation verification

Extensions of the model: Probability

• **Probabilistic views**
  ◊ Interface behavior: a probability distribution is given for the set of possible histories
  ◊ Architectural view: probability distributions for the sub-systems of the architecture
  ◊ State view: a probability distribution is given for the set of possible state transitions

• Then the model covers
  ◊ certain “non-functional properties” (safety, reliability, ...)
  ◊ Example: integrated fault trees

System Specification

Validation

Informal requirements

System delivery

System verification

R \Rightarrow S

S \leftarrow C_1 \otimes C_2 \otimes C_3

architecture design

Implementation

R = R_1 \otimes R_2 \otimes R_3

Integration

Component implementation

Verification R_1 \Rightarrow C_1 R_2 \Rightarrow C_2 R_3 \Rightarrow C_3

architecture verification

Summer School CPS Grenoble July 2013
Comprehensive System Architecture
Levels of Abstraction
Structuring Systems: levels of abstraction

<table>
<thead>
<tr>
<th>Anforderungen</th>
<th>Safety</th>
<th>Priority</th>
<th>Component</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>R_1</td>
<td>Yes</td>
<td>High</td>
<td></td>
<td></td>
</tr>
<tr>
<td>R_2</td>
<td>No</td>
<td>medium</td>
<td></td>
<td></td>
</tr>
<tr>
<td>R_n</td>
<td>no</td>
<td>low</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Goals and Requirements and Functional Specification
Model based Requirements Engineering

- A system development starts with a set of Goals $G$
- Derives from the goals $G$ Requirements $R$
- Derives from the requirements $R$ Specification $S$

Remarks:
- This can be seen as a refinement
- We need particular models to model goals, requirements, specifications
Relational view: Tracing – The power of logics

<table>
<thead>
<tr>
<th>Function</th>
<th>Safety</th>
<th>Priority</th>
<th>Component</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>A_1</td>
<td>...</td>
<td>Yes</td>
<td>high</td>
<td></td>
</tr>
<tr>
<td>A_2</td>
<td>...</td>
<td>No</td>
<td>medium</td>
<td></td>
</tr>
<tr>
<td>A_n</td>
<td>...</td>
<td>no</td>
<td>low</td>
<td></td>
</tr>
</tbody>
</table>

Domain and Context Modeling
System and its context
System and context

• How to model context?

• Systems in the context are systems that can be described again by their interface specification.
A safety view onto a system and its context

No Hazard:

\[ \text{OC} \land \text{SuC} \Rightarrow \text{No}_\text{Incident} (\text{CO}) \]
Moving scopes: Context view

System Spec:

\[ \text{SuC} \equiv (\text{OC} \Rightarrow \text{CO}) \]
Moving scopes: System interface view

SoC

System under Consideration
Moving scopes: Architectural view

Architecture Spec:
\[ A \land B \land C \land D \land E \land F \]

Architecture Correctness
\[ A \land B \land C \land D \land E \land F \Rightarrow SuC \]
Moving scopes: Sub-system view

Sub-system Spec:
\[ A \equiv (B \land C \land D \land E \land F \implies \text{SuC}) \]
Moving scopes:
Sub-system view

Sub-System under Consideration
Process

Operational Context

User Interface

Physical and technical context

System under Consideration

Context observations

System level glass box view
Example: Variations on the Scope

Interface behaviour of the “outer” system:

\[ \text{CPS} = \text{S/A} \otimes \text{LSK} \otimes \text{PRC} \otimes \text{MMI} \]

Interface behaviour of the inner system:

\[ \text{LSK} \]

The architecture of the system:

\[ \text{SYS} = \text{PHYC} [\times] \text{USER} [\times] \text{SURSYS} [\times] \text{CPS} \]

Three different system scopes and two different contexts

- The empty context for \( \text{SYS} \)
- The physical context, the user, surrounding system for the CPS
- The (sensor/actuator \( \otimes \) physical context), the (MMI \( \otimes \) User) and the (protocol \( \otimes \) surrounding-system) for the logical system kernel
Glass Box Specification of a Car´s Architecture

Car
∀ t: ¬ doors_closed(t) ⇒ act_speed(t) = 0

act_speed : Real

Motor
ready : Bool

WatchDog
doors_closed : Bool

Watch-Dog
assumption:
∀ t: ¬ ready(t) ⇒ act_speed(t) = 0

commitment:
∀ t: ¬ doors_closed(t) ⇒ act_speed(t) = 0

Example: how A/P-specifications can be formulated

• The specification
  \[ \forall t: \neg \text{doors\_closed}(t) \Rightarrow \text{act\_speed}(t) = 0 \]
can only be guaranteed if the two inner components work together. This requires
  \[ \forall t: \neg \text{ready}(t) \Rightarrow \text{act\_speed}(t) = 0 \]
• Then the system specification holds if
  \[ \forall t: \neg \text{doors\_closed}(t) \Rightarrow \neg \text{ready}(t) \]
• This is logically equivalent to the A/P-specification for the **WatchDog** assumption:
  \[ \forall t: \neg \text{ready}(t) \Rightarrow \text{act\_speed}(t) = 0 \]
  commitment: \[ \forall t: \neg \text{doors\_closed}(t) \Rightarrow \text{act\_speed}(t) = 0 \]
• In other words,
  ◊ the overall system specification can be guaranteed by the **watchdog**
  ◊ only if the assumption about the behaviour of the component **motor** holds.
Assumption/Promise to define Architectural Design Patterns

• A/P-specification

**assumption:** $\forall t: \neg \text{ready}(t) \Rightarrow \text{act\_speed}(t) = 0$

**commitment:** $\forall t: \neg \text{doors\_closed}(t) \Rightarrow \text{act\_speed}(t) = 0$

is logically guaranteed by the simple specification

$\forall t: \neg \text{doors\_closed}(t) \Rightarrow \neg \text{ready}(t)$

• This assertion no longer speaks about the specification of the environment, but is a pure interface specification.

• The example shows the simplification of an A/P-specification to a plain interface assertion.
Conclusion A/C

- A/C specs address the logic of the architecture rather than separated interface specifications
- From A/C specs we may derive simplified component specs
- This gives a methodology towards a modular decomposition
Key Principles in Engineering CPSs

- Abstraction
  - Interfaces
  - Changing levels of abstractions
- Modularity
  - Of composition
  - Of refinement
- Semantic coherence
  - From state machines to interfaces
  - From architectures to interfaces
  - From architectures of state machines to state machines of architectures
  - Probabilistic extension of logical (deterministic) models
- Multimodal representation
  - Denotational: mathematical models (of behavior)
  - Logical: specification and verification
  - Graphical: diagrams
  - Probabilistic: probability distributions on behavior
Concluding Remarks

- **The modelling framework Focus**
  - originally worked out for model based development
  - specification
  - verification
  - tool support
  See: https://af3.fortiss.org/projects/autofocus3

- **Tool: Autofocus 3**

- **Also useful for semantic foundation following the same approach**
  - SDL
  - Bus Systems: CAN, FLEXRAY
  - UML/SysML
  - SOA
Concluding Remarks

• Today software & systems engineering is too much orientated towards the technical architecture and solutions/implementation in the beginning
• We need a comprehensive “architectural” model-based view onto systems including requirements for dealing with complex multi-functional systems
• The models allow for
  ◊ Separation of concerns
  ◊ Separation of technical aspects from application aspects
• Technical architectures are modelled along the same theory
• Code and test cases can be generated from the models
The power of generalizing ideas, of drawing comprehensive conclusions from individual observations, is the only acquirement, for an immortal being, that really deserves the name of knowledge.

“Mary Wollstonecraft (1759–1797), British feminist. A Vindication of the Rights of Woman, ch. 4 (1792)