Verifiable and Resource-Aware Component-based Device Model for IoT

Youakim Badr

INSA-Lyon, LIRIS, France

youakim.badr@insa-lyon.fr

Context: IoT Challenges

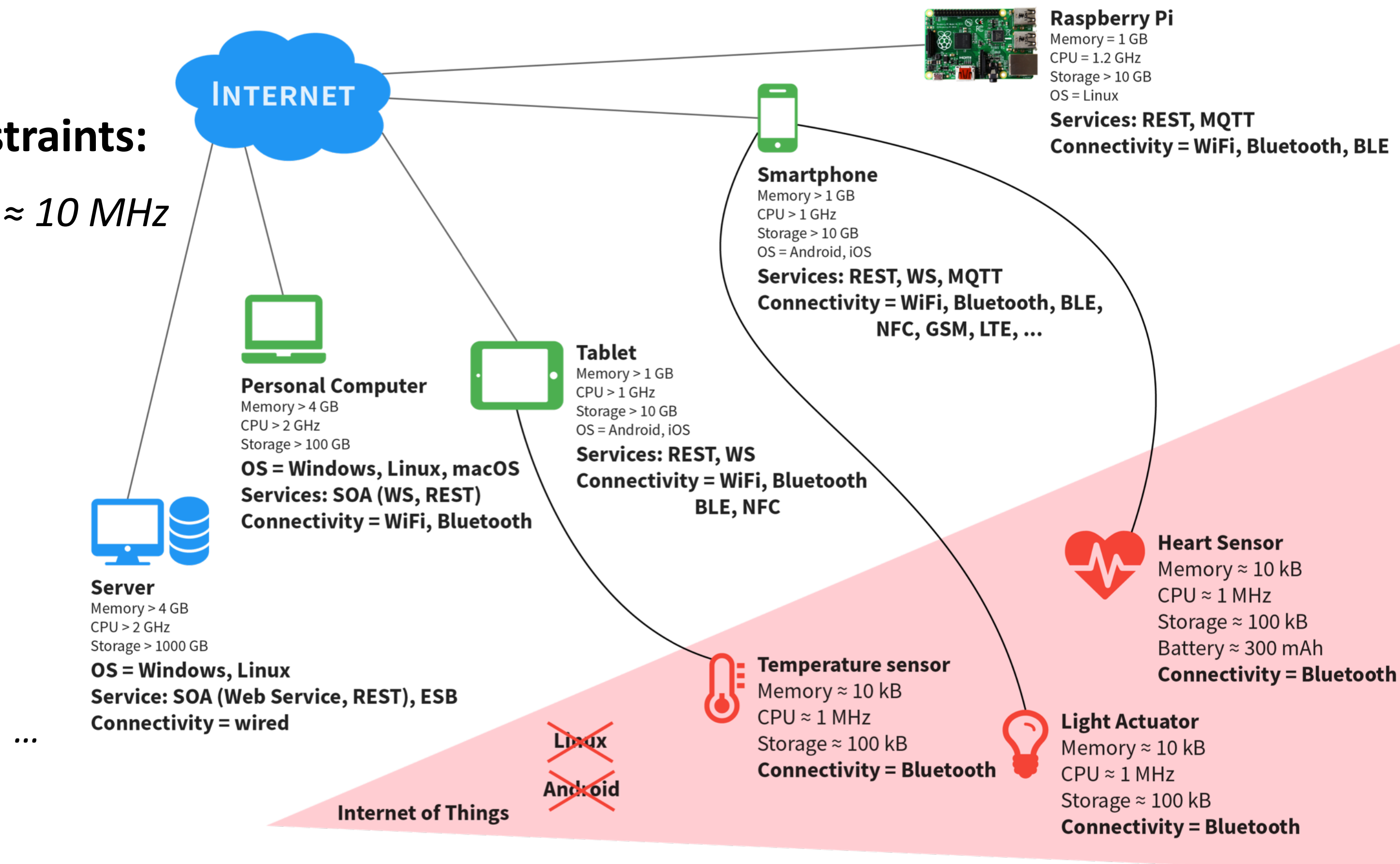
CHALLENGES

- **Interconnection** of **physical-world** devices

- Strong **hardware constraints:**

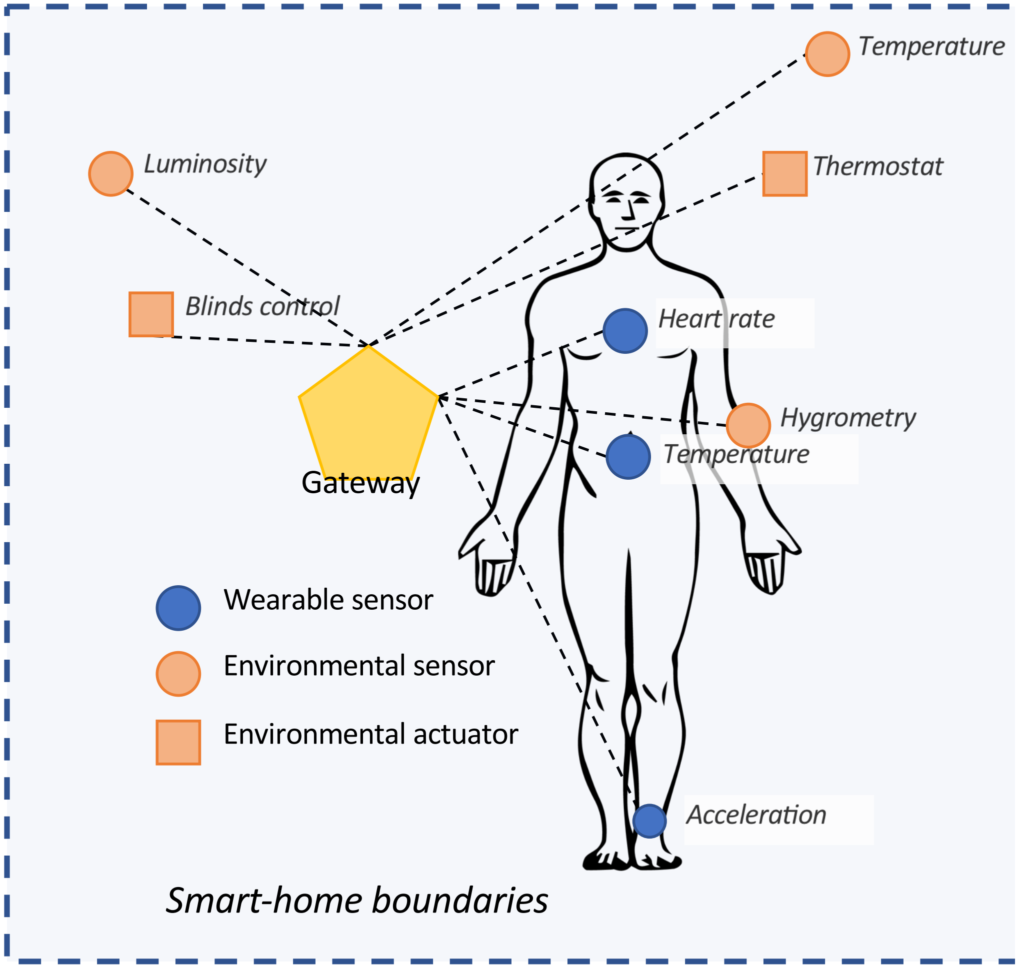
  - CPU frequency ≈ 10 MHz
  - RAM ≈ 10 kB
  - ROM ≈ 100 kB

- **Interoperability**
  - Bluetooth LE
  - Zigbee
  - IEEE 802.15.4



Motivation case-study

- Home automation for e-Health:
  - **Patient** equipped with **resource constrained wearable sensors**
  - **House** equipped with **environmental sensors** and **actuators**
  - **Computationally unlimited** central **gateway** used for composition

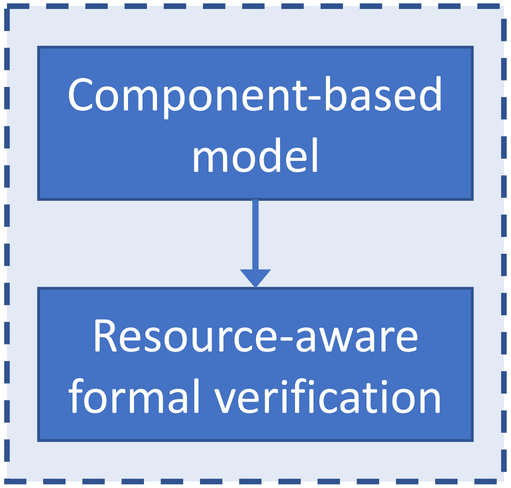


Problematic

How to build smart objects "**as a combination**" of sensors, controllers, actuators, physical things, taking into account resources

1. **Reusable** component based model:
   - information models, services and a lifecycle
   - cyber-physical properties
   - limited and consumable resources

2. **Resource-aware** verification framework



Comprehensive framework to build smart-objects as a combination of connected devices

Reusability in service computing

Services in SOA

- Agnostic
- Loosely coupled
- Remotely executable

Devices in IoT

- Reusable
- Modular
- Scalable

= SOA answers **some** of the concerns of the IoT

Services in SOA

- Pure programs
- Separation between data and their processing

Devices in IoT

- Hybrid SW/HW
- Self-contained and interoperable

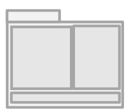
= SOA **must be adapted** to accurately model IoT Devices

= Logical-based Framework for Devices

Logical-based Framework for Smart Devices

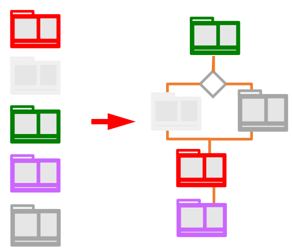
Composable, adaptable and resource-aware connected devices

IoT



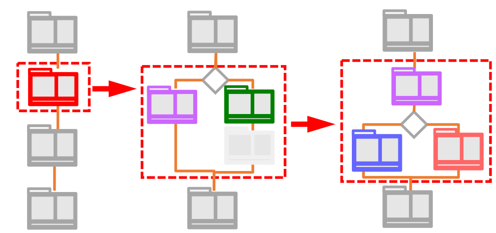
Specification

- Resources
- Contraintes



Composition

- Service Composition
- Composition of connected devices



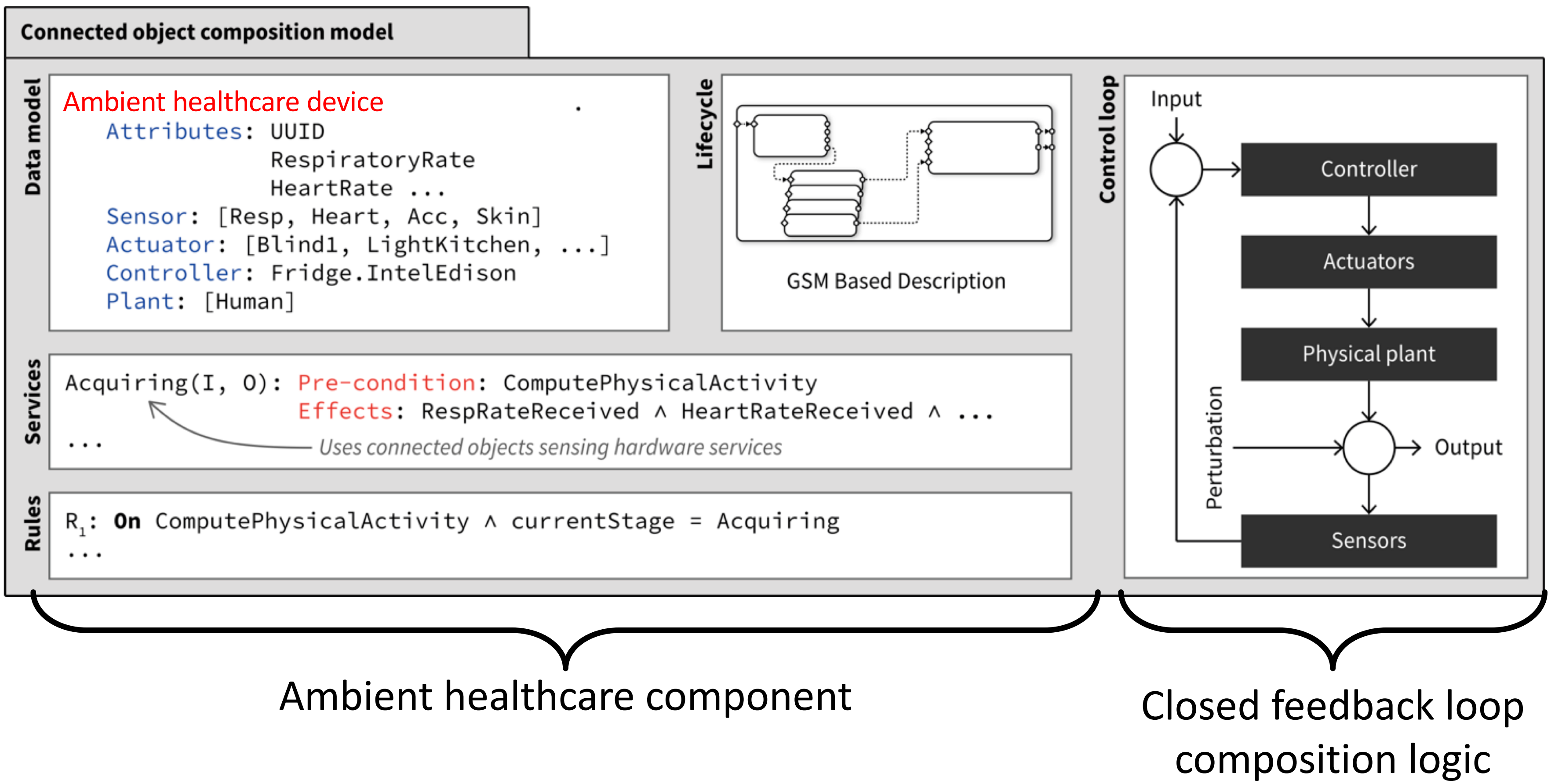
Self-Adaptable

- Small scale
- Large scale

Challenges

Validation/Verification	Automated and correct	Safety
- Liveness of bounded ressources - Artifact Verification (indecidabe) [Bhattacharya et al. BPM 07]	- Structural Contraints, dependancy - Composition (N-Hard problem) [T. Yu ACM Y Trans on the Web, 2007]	- Dynamic Environment - Incomplete Information

Component-based Connected Device Model



Connected Device Specification (I)

A connected device $\mathbf{D_i}$ = *<id, R, Q, QoS, S>*

id is the identifier of the connected device $\mathbf{D_i}$.

R set of consumable **resources** : $R = R_v \cup R_r = \{r^n\} \cup \{r^{[n]}\}$

R_v is the set of vanishing resources
n=1, r^n is consumed one time
n>1, r^n is consumed more than one time (n is bounded)
n=!, r^n is consumed unlimited number of times (n is unbounded)

R_r is the set of renewal resources
n=1, $r^{[n]}$ is consumed at most n times (can be regenerated when disposed)

$S = \{s_1, s_2, \ldots\}$ is the set of services.
A service $s_i = < I \cup O, R, Q, QoS_i, E >$
$I = \{i_1, i_2 \ldots\}$, is a set of input messages $(\mathbf{i_i})$.
$O = \{o_1, o_2 \ldots\}$, is a set of output messages $(\mathbf{o_i})$.
E = is an exception

Q = set of states = $\{q_1, q_2, q_3, \ldots\}$

QoS = $<Q_1, Q_2, \ldots, Q_n>$ is the set of qualitative and quantitative QoS attributes $(\mathbf{q_i})$.

$$id \otimes R_v \otimes R_r \otimes Q \otimes I \multimap ((O \otimes R_r) \oplus E) \otimes Q$$

ECG sensor (E) : HR() → hr
HRV(hr300)→hrv={SSDN, RMSSD, LF-HF, NormLF}
buffer(hr, timestep) → hr300 // timestep global variable (context)

Actimetry sensor (A) : Activity() → activity = [running, walking, sleeping, sitting]

Electrodermal sensor (D) : Dermal() →srr // skin resistance response

MailServer (M) : send(addresses) →email

Phone (P) : send(riskLevel, phoneNumbers) → sms
call(RiskLevel, phoneNumber)→ voiceMsg

Inertial measurement unit (IMU): position(on) → (x, y, z)

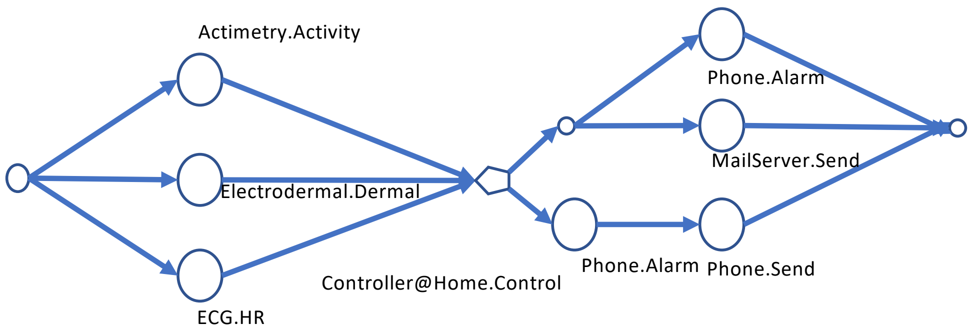
Occupancy sensor (O_1, … O_n) : presence(on) → (Ispresent, room)
PositionRoom(room) → (x, y, z)

Controller@Home (CH): Predit(hrv, activity, ?srr)→ riskLevel
Control(riskLevel, (x, y, z))→ Phone.call xor (?MailServer.send|| Phone.Alarm

Controller@Phone (CP): Predit(hrv, activity, srr)→ riskLevel
Control service: control(riskLevel, (x, y, z))→ [send || call || alarm] xor Mail.Send

Vanishing resources: R_v = {battery (200mAh), security certificate (expiration date), password (80 times), …}
Renewal resources: R_r = {memory (64Kb), bandwidth (100Mbs), … }
QoS = {response_time, cost(euros), concurrentRequests(capacity), throughput(latency/capacity), dataEncryption (y/n), Connectivity([BL | Wifi | wired]), Reliability, … }

Workflow of composite connected devices



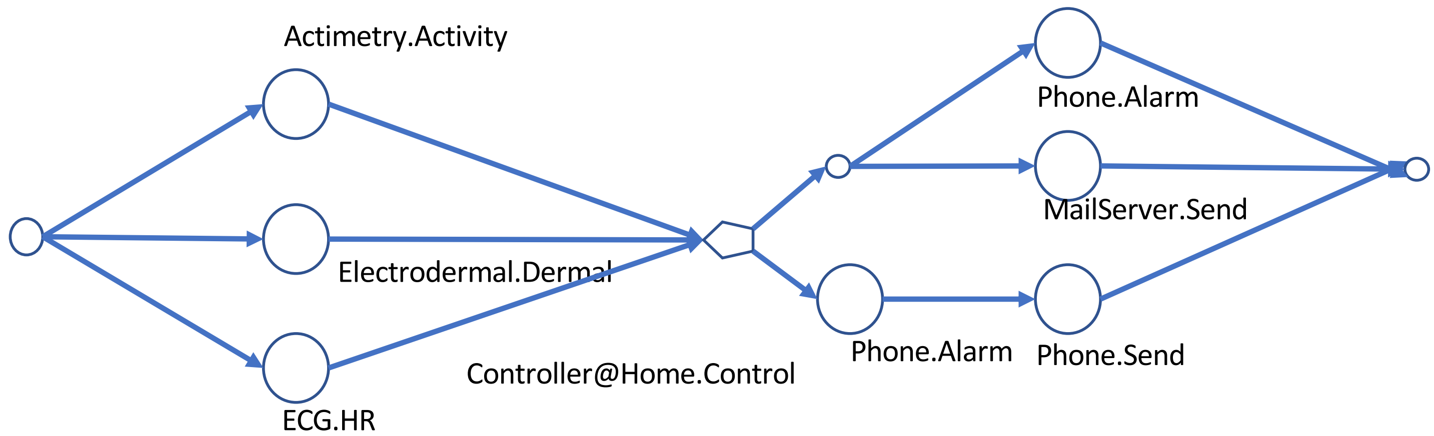
Composition Patterns

- Sequence Pattern: s_i ; s_j
- Parallel Pattern: *andSplit*(s_i , s_j , s_k)
- Selection Pattern: *xorSplit*[*condition*](s_i , s_j , s_k)
- Iteration Pattern: *iter*[*condition*](s_i)

```
BEGIN; andSplit(
    Actimetry.Activity()(activity),
    Electrodermal.Dermal()(srr),
    ECG.HR()(hr);
      seq[ECG.HR.hr = ECG.buffer.hr];
      ECG.buffer(hr, timestep)(hr300);
      seq[ECG.buffer.hr = ECG.HRV.hr300];
      ECG.HRV(hr300);
      xor[switch(context)(home ; outside)] (
                    ?home(
                                Controller@Home.Predict(hrv, activity, ?srr)( riskLevel);
                    seq[Controller@Home.Predict.riskLevel= Controller@Home.Control.riskLevel]);
                    Controller@Home.Control(riskLevel, (x, y, z))();
                                xorSplit[switch(SGM)(OK ; KO)](
                                            ?OK(
                                                        Phone.Call(RiskLevel, phoneNumbers)(voiceMsg)
                                                        ),

                                            ?KO(
                                                        andSplit(
                                                                    ?MailServer.Send(addresses)(email),
                                                                    Phone.Alarm(phoneNumber)(voiceMsg)),
                                                        andJoin(email, voiceMsg)
                                                        )
                                xorJoin(<voiceMsg> or < email, voiceMsg >)
                                ),
                    ?outside(
                    Controller@Phone.Predict(hrv, activity, ?srr)( riskLevel);
                    seq[Controller@Phone.Predict.riskLevel= Controller@Phone.Control.riskLevel]);
                    Controller@Phone.Control(riskLevel, (x, y, z))();
```

QoS Composite Connected Devices (II)



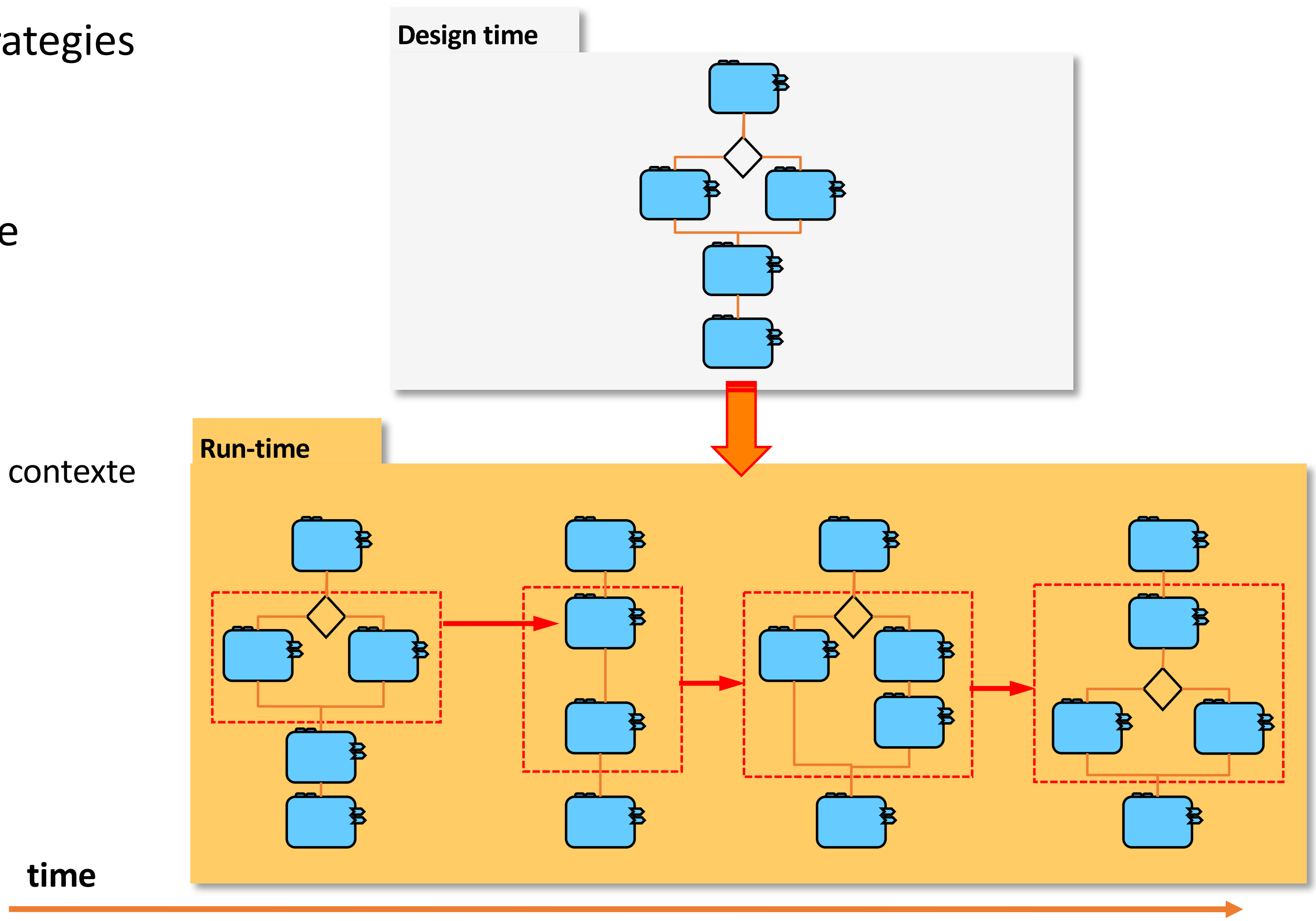
QoS Attribute Name	Measure Scales	Composition Pattern Calculation Methods			
		Sequence	Parallel	Condition	Iteration
connectivity(CO)	Nominal	$\bigcap_{i=1}^{n} co_i$	$\bigcap_{i=1}^{n} co_i$	$\bigcap_{i=1}^{n} co_i$	$\bigcap_{i=1}^{n} co_i$
Security (SE)	Ordinal	$min(se_i)$	$min(se_i)$	$min(se_i)$	$min(se_i)$
Rating Point (RP)	Interval	$min(rp_i)$	$min(rp_i)$	$min(rp_i)$	$min(rp_i)$
Response Time (RT)	Ratio	$\sum_{i=1}^{n} rt_i$	$max(rt_i)$	$max(rt_i)$	$rt*k$
Reliability (RE)	Ratio	$\prod_{i=1}^{n} re_i$	$\prod_{i=1}^{n} re_i$	$min(re_i)$	re^k
Price (P)	Ratio	$\sum_{i=1}^{n} p_i$	$\sum_{i=1}^{n} p_i$	$max(p_i)$	$p*k$

Composition Constraints (III)

- ***Structural constraints***
  - ECG.buffer; ECG.HRV
- ***Constraint constraints***
  - ***Local Constraints***
    - c_r = < Phone.battery , ⊉ , Low >
  - ***Global Constraints***
    - c_{rg} = <HeartAttac.response_time, <, 2 min>
- ***Dependency constraints***
  - *Preferred, Excluded, …*

Resilient connected object model (IV)

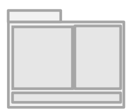
- Reactive vs proactive strategies
- Moving Target Technique
- Generation of Variants
  - Substitution
  - Replication
  - Contextual Variations du contexte
  - Topologies
    - Composition
    - Decomposition
    - …

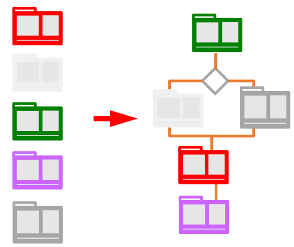


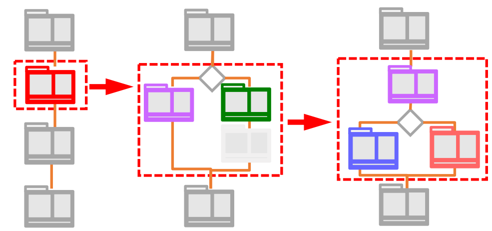
Logical-based Framework for Smart Devices

Composable, adaptable and resource-aware connected devices

IoT







Specification

- Resources
- Contraintes

Composition

- Service Composition
- Composition of connected devices

Self-Adaptable

- Small scale
- Large scale

Challenges

Validation/Verification	Automated and correct	Safety
- Liveness of bounded ressources - Artifact Verification (indecidabe) [Bhattacharya et al. BPM 07]	- Structural Contraints, dependancy - Composition (N-Hard problem) [T. Yu ACM Y Trans on the Web, 2007]	- Dynamic Environment - Incomplete Information

Logical-based Framework

Logical Frameworks: Abella, Beluga, Hybrid, Twelf, ...

Formal reasoning systems : Coq, Isabelle/HOL

Linear Logic [Girard 1986]: linprover, l2coq, llprover, TATU and Quati,

- Resource-aware lambda-calculus [Lafont 1993]
- Proofs-as-processes in RAPS (ILL) [Rao et al. 2006]
- Proofs-as-processes in HOL Light (CLL) [Papapanagiotou et al. 2011]
- Constraint programming [Rao et al. 2006]

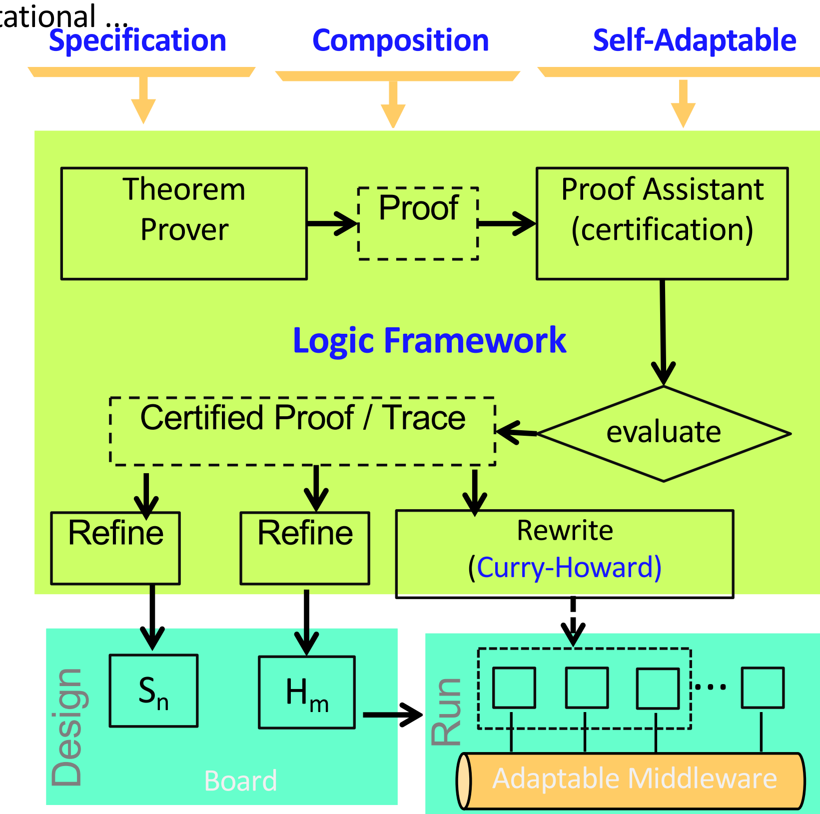
Logic-based Framework for Smart Devices

Composable, adaptable and resource-aware connected devices

- **Specification of bounded resources**
  - spatial and temporal resources, energy consumption, storage and computational ...
- **Constraints Specifications r w to all possible compositions**
  - inter-objets structural constraints, dependency, exclusion, ...
- **Automated theorem proving**
  - automated and correct Composition
    - Find a proof, satisfying constraints
    - Control search strategy
  - Adaptation and safety
    - Find all "possible" proofs (if possible)
- **Proofs Verification**
  - Proof-as-program (Curry-Howard)
    - Export certified proofs
- Formal Computational Specifications with **Subexponential** Logic

  - Specify **Subexponential logic framework**

  - Automate proof search (certify and export proof)



Verifiable composition – Taste of Linear Logic

- **Linear Logic (**J.Y. Girard 1986)
  - A::= P |A $\multimap$ A | A$\otimes$A | A$\oplus$A | A&A | !A | 1
- Antony Hoare (1985)'s Vending Machine example
  - **Linear Logic** : $\$1 \Rightarrow candy$
  - **Classical or Intuitionistic logic**
    - $(A$ and $A \Rightarrow B) \Rightarrow A \wedge B$
    - $(\$1$ and $\$1 \Rightarrow candy) \Rightarrow \$1 \wedge candy$
- **A Logic of Resources**
  - $A \multimap B$ = transform resource A into resource B

    $\$1 \multimap candy$
  - $A \otimes B$ = **Multiplicative conjunction** consumes simultaneous resources

    $\$3 \multimap (candy \otimes chips \otimes drink)$ // $\$3 := \$1 \otimes \$1\ \$1$

    $\$1 \multimap (candy \otimes chips \otimes drink)$ // wrong
  - $A \& B$ = **Additive conjunction** represents alternative occurrence of resources

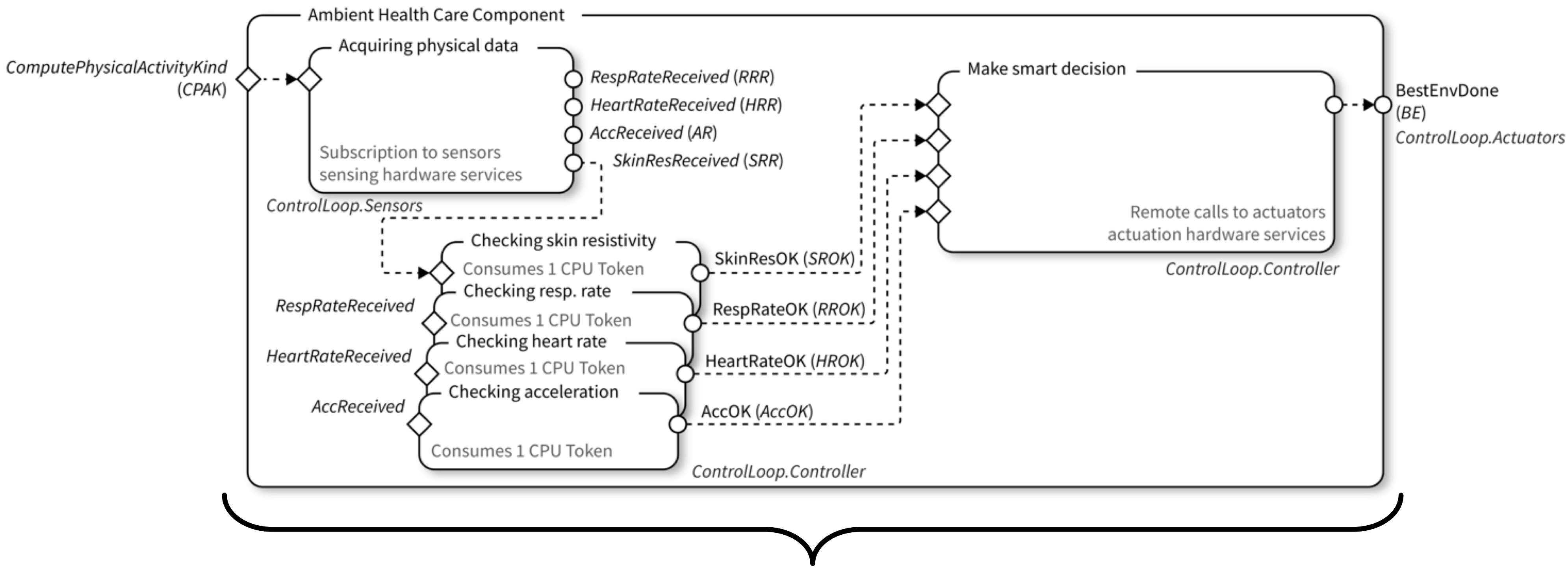
    $\$1 \multimap (candy \& chips \& drink)$

    $\$3 \multimap (candy \& chips \& drink)$
  - $A \oplus B$ = **Additive disjunction** represents alternative occurrence of resources

    $\$1 \multimap (candy \oplus chips \oplus drink)$.

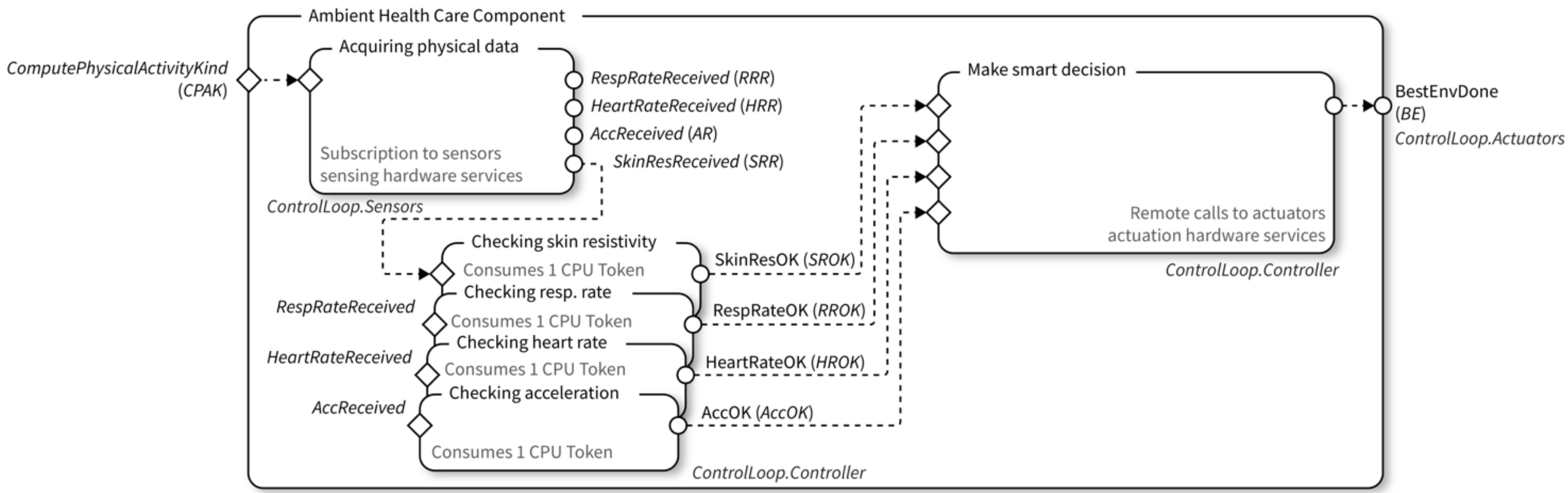
Composite devices (wf) in GSM model

- Lifecycle:
  - **Guards:** entry point of a stage.
  - **Stage body:** contains one or multiple services.
  - **Milestones:** events that deactivates the stage body.



Ambient healthcare component lifecycle derived from the composition of multiple sensors

Encoding GSM with linear logic



acquiring: $CPAK \vdash RRR \otimes HRR \otimes AR \otimes SRR$

checkingSR: $CPU \otimes SRR \vdash SROK$

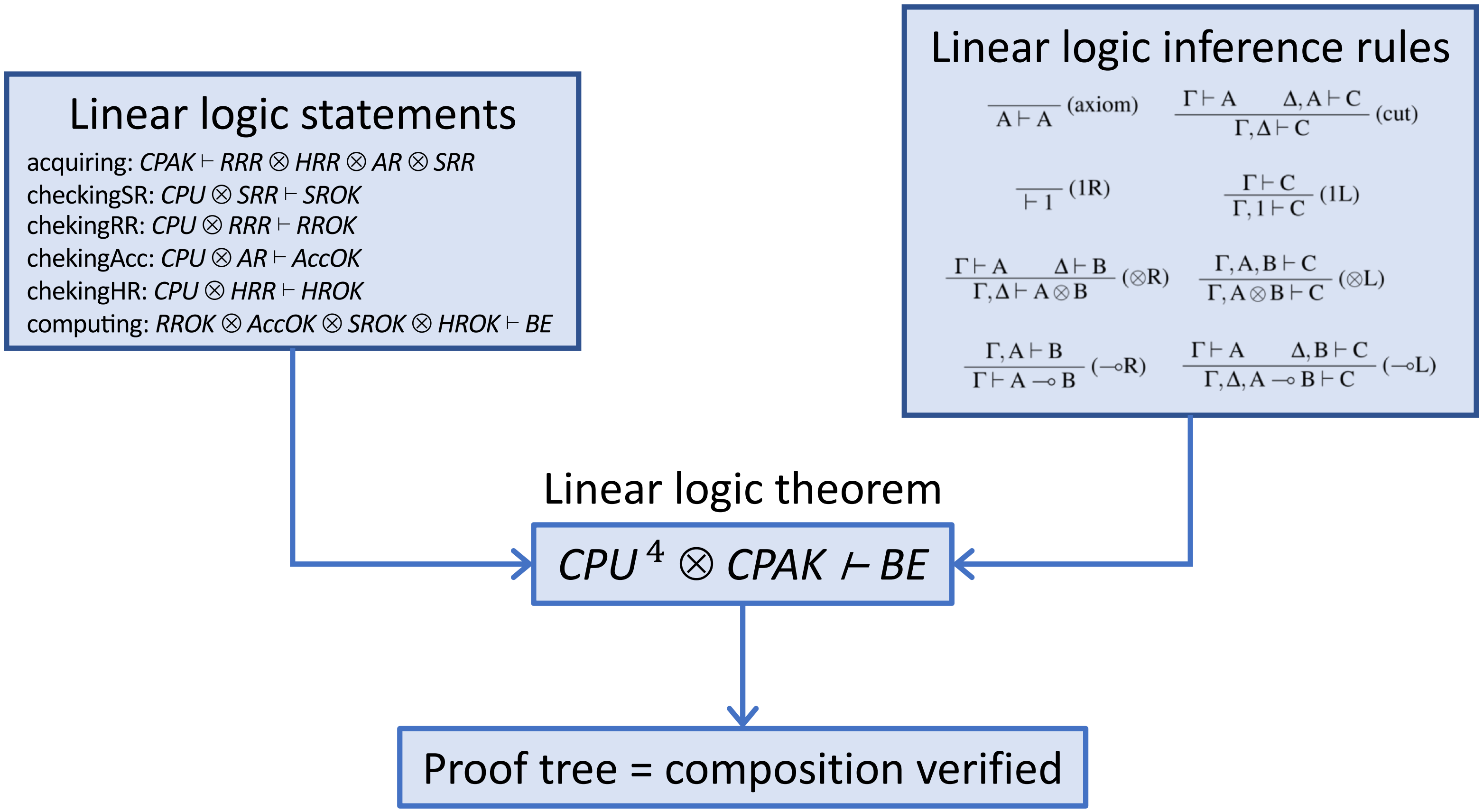
chekingRR: $CPU \otimes RRR \vdash RROK$

chekingAcc: $CPU \otimes AR \vdash AccOK$

chekingHR: $CPU \otimes HRR \vdash HROK$

computing: $RROK \otimes AccOK \otimes SROK \otimes HROK \vdash BE$

Verifiable composition



LL Proof

- The theorem to be proven is: $CPU^4 \otimes CPAK \vdash BE$

- The proof tree of the ambient healthcare composite component is:

$$\dfrac{\text{(checkingAcc)}}{CPU \otimes AR \vdash AccOK} \qquad \dfrac{\text{(checkingHR)}}{CPU \otimes HRR \vdash HROK}$$

$$\dfrac{CPU \otimes AR \vdash AccOK \qquad CPU \otimes HRR \vdash HROK}{CPU \otimes AR, CPU \otimes HRR \vdash AccOK \otimes HROK}\ (\otimes R)$$

$$\dfrac{CPU \otimes AR, CPU \otimes HRR \vdash AccOK \otimes HROK}{CPU^2 \otimes AR \otimes HRR \vdash AccOK \otimes HROK}\ (\otimes L)$$

$$\dfrac{\dfrac{\text{(checkingSR)}}{CPU \otimes SRR \vdash SROK} \qquad CPU^2 \otimes AR \otimes HRR \vdash AccOK \otimes HROK}{CPU \otimes SRR, CPU^2 \otimes AR \otimes HRR \vdash SROK \otimes AccOK \otimes HROK}\ (\otimes R)$$

$$\dfrac{CPU \otimes SRR, CPU^2 \otimes AR \otimes HRR \vdash SROK \otimes AccOK \otimes HROK}{CPU^3 \otimes SRR \otimes AR \otimes HRR \vdash SROK \otimes AccOK \otimes HROK}\ (\otimes L)$$

$$\dfrac{\dfrac{\text{(checkingRR)}}{CPU \otimes RRR \vdash RROK} \qquad CPU^3 \otimes SRR \otimes AR \otimes HRR \vdash SROK \otimes AccOK \otimes HROK}{CPU \otimes RRR, CPU^3 \otimes SRR \otimes AR \otimes HRR \vdash RROK \otimes SROK \otimes AccOK \otimes HROK}\ (\otimes R)$$

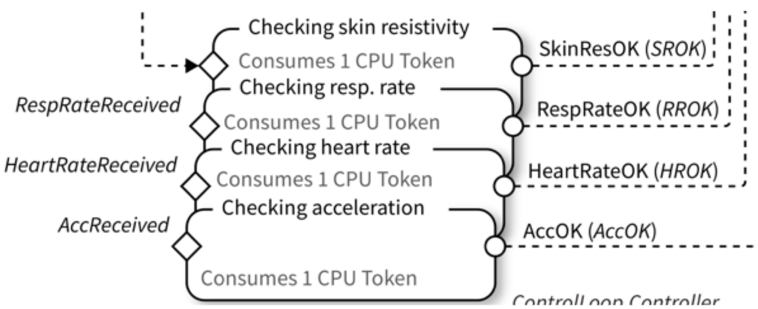
$$\dfrac{CPU \otimes RRR, CPU^3 \otimes SRR \otimes AR \otimes HRR \vdash RROK \otimes SROK \otimes AccOK \otimes HROK}{CPU^4 \otimes RRR \otimes SRR \otimes AR \otimes HRR \vdash RROK \otimes SROK \otimes AccOK \otimes HROK}\ (\otimes L)$$

$$\dfrac{\dfrac{\text{(acquiring)}}{CPAK \vdash RRR \otimes SRR \otimes AR \otimes HRR} \qquad CPU^4 \otimes RRR \otimes SRR \otimes AR \otimes HRR \vdash RROK \otimes SROK \otimes AccOK \otimes HROK}{CPU^4 \otimes CPAK \vdash RROK \otimes SROK \otimes AccOK \otimes HROK}\ (cut)$$

$$\dfrac{CPU^4 \otimes CPAK \vdash RROK \otimes SROK \otimes AccOK \otimes HROK \qquad \dfrac{\text{(computing)}}{RROK \otimes SROK \otimes AccOK \otimes HROK \vdash BE}}{CPU^4 \otimes CPAK \vdash BE}\ (cut)$$

Proof tree interpretation

- Proof tree can further be interpreted in terms of composition:
  - The *cut* rule corresponds to the serial composition of stages.
  - The $\otimes R$ and $\otimes L$ rules correspond to the parallel composition of stages.



$$\frac{\dfrac{\text{(checkingAcc)}}{CPU \otimes AR \vdash AccOK} \quad \dfrac{\text{(checkingHR)}}{CPU \otimes HRR \vdash HROK}}{CPU \otimes AR, CPU \otimes HRR \vdash AccOK \otimes HROK}\ (\otimes R)$$

$$\frac{CPU \otimes AR, CPU \otimes HRR \vdash AccOK \otimes HROK}{CPU^2 \otimes AR \otimes HRR \vdash AccOK \otimes HROK}\ (\otimes L)$$

$$\frac{\dfrac{\text{(checkingSR)}}{CPU \otimes SRR \vdash SROK} \quad CPU^2 \otimes AR \otimes HRR \vdash AccOK \otimes HROK}{CPU \otimes SRR, CPU^2 \otimes AR \otimes HRR \vdash SROK \otimes AccOK \otimes HROK}\ (\otimes R)$$

$$\frac{CPU \otimes SRR, CPU^2 \otimes AR \otimes HRR \vdash SROK \otimes AccOK \otimes HROK}{CPU^3 \otimes SRR \otimes AR \otimes HRR \vdash SROK \otimes AccOK \otimes HROK}\ (\otimes L)$$

$$\frac{\dfrac{\text{(checkingRR)}}{CPU \otimes RRR \vdash RROK} \quad CPU^3 \otimes SRR \otimes AR \otimes HRR \vdash SROK \otimes AccOK \otimes HROK}{CPU \otimes RRR, CPU^3 \otimes SRR \otimes AR \otimes HRR \vdash RROK \otimes SROK \otimes AccOK \otimes HROK}\ (\otimes R)$$

$$\frac{CPU \otimes RRR, CPU^3 \otimes SRR \otimes AR \otimes HRR \vdash RROK \otimes SROK \otimes AccOK \otimes HROK}{CPU^4 \otimes RRR \otimes SRR \otimes AR \otimes HRR \vdash RROK \otimes SROK \otimes AccOK \otimes HROK}\ (\otimes L)$$

Q /A