
Feng Tan*, Yufei Wang*, Qixin Wang*, Lei Bu†, Rong Zheng‡, Neeraj Suri**

* Embedded Systems & Networking Lab, Dept. of Computing, The Hong Kong Polytechnic Univ.
† State Key Lab for Novel Software Tech., Dept. of Computer Sci. & Tech., Nanjing Univ., China
‡ Dept. of Computing and Software, McMaster Univ., Canada
** Dept. of Computer Science, TU Darmstadt, Germany

June 26, 2013
Cyber-Physical Systems (CPS) are typically distributed and life/mission critical.

Life/Mission critical CPS demand wireless

Conflict

Wireless is unreliable
Cyber-Physical Systems (CPS) are typically distributed and life/mission critical.

Life/Mission critical CPS demand wireless

Wireless is unreliable

Conflict

PTE Safety Guarantee
Cyber-Physical Systems (CPS) are typically distributed and life/mission critical.

Life/Mission critical CPS demand wireless.

Wireless is unreliable.

Conflict

Design Pattern
Hybrid Modeling

PTE Safety Guarantee
Cyber Physical Systems (CPS): systems involving tight/complex coupling of computer and physical subsystems

Avionics

Manufacturing

Medical
CPS Features

Typically distributed and life/mission-critical

Real-time (in addition to logical time) matters

Modeling must integrate both discrete and continuous aspects
Distributed life/mission critical CPS demand wireless communications.
Distributed life/mission critical CPS demand wireless communications.
Distributed life/mission critical CPS demand wireless communications.
Distributed life/mission critical CPS demand wireless communications.

Wireless is unreliable
How to guarantee the safety of life/mission critical wireless CPS?

Life/Mission critical CPS demand wireless

Conflict

Wireless is unreliable
How to guarantee the Proper-Temporal-Embedding (PTE) safety rule of life/mission critical wireless CPS?

Life/Mission critical CPS demand wireless

Conflict

Wireless is unreliable

PTE Safety Guarantee
What is Proper-Temporal-Embedding (PTE) safety rule?
CPS Feature 2: real-time (in addition to logical time) matters!
CPS Feature 2: real-time (in addition to logical time) matters!

- **Laser-scalpel**
- **(O_2) ventilator**

- **t 1**
- **t 2**
- **t 3**
- **t 4**

- **Time**

- **emission**
- **shutoff**
- **pause**
- **ventilating**

**risky state dwelling**

**time upper bound**
CPS Feature 2: real-time (in addition to logical time) matters!
CPS Feature 2: real-time (in addition to logical time) matters!

- Laser-scalpel
- \((O_2)\) ventilator

\[ t_1 \quad t_4 \quad t_2 \]

- emission
- shutoff
- pause
- ventilating

Time

exit-risky safeguard interval
How to guarantee PTE safety despite of arbitrary wireless link failures?

![Diagram showing time intervals for laser scalpel and oxygen ventilator operations.](image-url)
How to guarantee PTE safety despite arbitrary wireless link failures?

**Leasing Design Pattern:**

risky state dwelling time must be leased.
General concepts of Leasing design pattern: each CPS entity takes one of the 3 roles.

1. request
2. lease
3. approve

Initiator
Supervisor
Participant
CPS Features: 1. real-time matters; 2. real-time PTE even when aborting/canceling. (+ 3. arbitrary comm. failures)
How to formally describe, analyze, and use Leasing design pattern in the context of CPS?
How to formally describe, analyze, and use Leasing design pattern in the context of CPS?

CPS Feature 3 implies the use of hybrid automata modeling.
Hybrid Automaton is a state-of-the-art modeling tool for CPS.

Bouncing Ball Example

Free fall $\dot{y} = -g$

Collision $y^+(t) = y^-(t) = 0$

$\dot{y}^+(t) = -cy^-(t)$

for any $c < 1$, there are infinitely many transitions in finite time (Zeno phenomena)

Guard or jump condition

$x_1 = 0 \& x_2 < 0$?

Transition

State reset

$x_2 := -c x_2^-$
Leasing Design Pattern for PTE Safety Rules: detailed Supervisor's hybrid automaton
Leasing Design Pattern for PTE Safety Rules:
detailed Initiator's hybrid automaton

**Fall-Back**

- **Exiting 1:**
  \[ \dot{t}_{clk} = 1; \]
  \[ 0 \leq t_{clk} < T_{exit,N} \]

- **Risky Core:**
  \[ \dot{t}_{clk} = 1; \]
  \[ 0 \leq t_{clk} < T_{run,N} \]

- **Entering:**
  \[ \dot{t}_{clk} = 1; \]
  \[ 0 \leq t_{clk} < T_{enter,N} \]

**Requesting:**

- \[ \dot{t}_{clk} = 1; \]
  \[ 0 \leq t_{clk} < T_{req,N} \]

**Events:**

- `!evt_\xi_0 To_\xi_0 Req`: \[ t_{clk} \leftarrow 0. \]
- `evt_Req_Expire`: \[ t_{clk} \geq T_{max} \]
- `!evt_\xi_0 To_\xi_0 Cancel`: \[ 0 \leq t_{clk} < T_{max} \]
- `evt_\xi_0 Enter`: \[ t_{clk} \leftarrow 0. \]
- `!!evt_\xi_0 To_\xi_0 Approve`: \[ t_{clk} \leftarrow 0. \]
- `!!evt_\xi_0 To_\xi_0 Abort`: \[ t_{clk} \leftarrow 0. \]
Leasing Design Pattern for PTE Safety Rules: detailed Participant's hybrid automaton

**Exiting 1:**
\[ t_{clk} = 1; \]
\[ 0 \leq t_{clk} < T_{exit,i} \]

**Exiting 2:**
\[ t_{clk} = 1; \]
\[ 0 \leq t_{clk} < T_{exit,i} \]

**Risky Core:**
\[ t_{clk} = 1; \]
\[ 0 \leq t_{clk} < T_{max}^{run,i} \]

**Entering:**
\[ t_{clk} = 1; \]
\[ 0 \leq t_{clk} < T_{max}^{enter,i} \]

**Fall-Back**

- **LeaseReq**
- **LeaseDeny**
- **LeaseApprove**

[ParticipationCondition]
Leasing Design Pattern for PTE Safety Rules: detailed Participant's hybrid automaton

Exitting 1: 
\[ t_{clk} = 1; \]
\[ 0 \leq t_{clk} < T_{exit,i} \]

Risky Core: 
\[ t_{clk} = 1; \]
\[ 0 \leq t_{clk} < T_{max,run,i} \]

Entering: 
\[ t_{clk} = 1; \]
\[ 0 \leq t_{clk} < T_{max,enter,i} \]

Intermediate Location btw two events. Cost 0 time.
Leasing Design Pattern for PTE Safety Rules: detailed Participant's hybrid automaton
Theorem 1: If the temporal parameters of the design pattern hybrid automata satisfy a certain set of linear inequalities, then PTE safety is guaranteed despite of arbitrary communications link failures.
Validity of the design pattern

c1. All configuration time constants \((T_{\text{wait}}^{\text{max}}, T_{\text{fb},0}^{\text{min}}, T_{\text{LS1}}^{\text{max}}, T_{\text{req},N}^{\text{max}}, T_{\text{enter},i}^{\text{max}}, T_{\text{run},i}^{\text{max}}, T_{\text{exit},i}^{\text{max}}, \text{where } i = 1 \sim N)\) are positive.

c2. \(T_{\text{LS1}}^{\text{max}} \triangleq T_{\text{enter},1}^{\text{max}} + T_{\text{run},1}^{\text{max}} + T_{\text{exit},1}^{\text{max}} > NT_{\text{wait}}^{\text{max}}.\)

c3. \((N - 1)T_{\text{wait}}^{\text{max}} < T_{\text{req},N}^{\text{max}} < T_{\text{LS1}}^{\text{max}}.\)

c4. \(\forall i \in \{1, 2, \ldots, N\}, \) there is
\[
(i - 1)T_{\text{wait}}^{\text{max}} + T_{\text{enter},i}^{\text{max}} + T_{\text{run},i}^{\text{max}} + T_{\text{exit},i}^{\text{max}} \leq T_{\text{LS1}}^{\text{max}}.
\]

c5. \(\forall i \in \{1, 2, \ldots, N - 1\}, \) there is
\[
T_{\text{enter},i}^{\text{max}} + T_{\text{run},i}^{\text{max}} + T_{\text{exit},i}^{\text{max}} < T_{\text{enter},i+1}^{\text{max}}.
\]

c6. \(\forall i \in \{1, 2, \ldots, N - 1\}, \) there is
\[
T_{\text{enter},i}^{\text{max}} + T_{\text{run},i}^{\text{max}} > T_{\text{wait}}^{\text{max}} + T_{\text{enter},i+1}^{\text{max}} + T_{\text{run},i+1}^{\text{max}} + T_{\text{exit},i+1}^{\text{max}}.
\]

c7. \(\forall i \in \{1, 2, \ldots, N - 1\}, \) there is \(T_{\text{exit},i}^{\text{max}} > T_{\text{safe},i+1 \rightarrow i}^{\text{min}}.\)
Using the design pattern: how to turn design pattern into detailed CPS designs?
We proposed a formal procedure to elaborate a design pattern hybrid automaton into a detailed design hybrid automaton.
Validity of elaboration

Theorem 2: If detailed design hybrid automata are respectively derived by elaborating corresponding design pattern hybrid automata, then PTE safety is guaranteed despite of arbitrary communications link failures.
Laser Tracheotomy Medical CPS: interconnect/interlock smart medical devices to increase safety

Laser Tracheotomy without Device Interlock
Laser Tracheotomy Medical CPS: interconnect/interlock smart medical devices to increase safety
Demand to use wireless links for safety and efficiency concerns.
Demand to use wireless links for safety and efficiency concerns.
Demand to use wireless links for safety and efficiency concerns.
Laser Tracheotomy CPS PTE safety rule.

- Laser-scalpel
- \((O_2)\) ventilator

- \(t_1\) ≥ 3 sec
- \(t_4\) ≤ 60 sec
- \(t_2\) ≥ 1.5 sec
System architecture and roles of the design pattern: Initiator, Supervisor, Participant
System architecture and roles of the design pattern: **Initiator**, Supervisor, Participant
System architecture and roles of the design pattern: Initiator, Supervisor, Participant
System architecture and roles of the design pattern: Initiator, Supervisor, Participant

![Diagram showing system architecture with roles Initiator, Supervisor, Participant and components such as SpO₂ Sensor, Ventilator, and Laser Scalpel]
Following the Leasing design pattern and Elaboration procedure, we derive detailed designs.
Emulation Scheme

- Human Subject (HS)
- SpO₂
- Supervisor
- Wired Connection
- Wireless Connection
- Laser-Scalpel
- Interference Source

Connections:
- 0.3 m between Human Subject and Supervisor
- 0.3 m between Supervisor and Laser-Scalpel

## Emulation Results

<table>
<thead>
<tr>
<th>Trial Mode</th>
<th>$E(T_{off})$ (sec)</th>
<th># of Laser Emissions</th>
<th># of Failures</th>
<th># of $evtToStop$</th>
</tr>
</thead>
<tbody>
<tr>
<td>with Lease</td>
<td>18</td>
<td>19</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>without Lease</td>
<td>18</td>
<td>11</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>with Lease</td>
<td>6</td>
<td>19</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>without Lease</td>
<td>6</td>
<td>12</td>
<td>3</td>
<td>0</td>
</tr>
</tbody>
</table>

1. Each trial lasts 30 minutes, and is under constant WiFi interference.
2. For each trial, the expectation $E(T_{on}) \equiv 30$(sec).
3. $evtToStop$ occurs when lease expiration forces the laser-scalpel to stop emitting (see Fig. 12), i.e. when lease mechanism takes effect to rescue the system from violating the PTE safety rules.
Related Work

Leasing Protocol [7,8,9,10,11,12][24]

check-point & roll-back

logical time vs. real-time PTE

uncontrollable physical world parameters
Related Work

Use of formal modeling in design pattern [30~33].

Hybrid modeling mostly used for verification [3],[13~16].

Tichakorn [34] proposes use a subclass of hybrid automata for designing periodical hybrid control systems.
Conclusion

1. Proposed a Lease based design pattern to guarantee PTE safety rules in wireless CPS, under arbitrary communication link failures.

2. Derived the corresponding closed-form linear constraints for temporal configuration parameters.

3. Formal description of design pattern with hybrid modeling.

4. Proposed a formal methodology to elaborate design pattern hybrid automata to detailed design hybrid automata, while maintaining PTE safety properties.
Thank you!

Life/Mission critical CPS demand wireless

Conflict

Design Pattern
Hybrid Modeling

PTE Safety Guarantee

Wireless is unreliable
Cyber Physical Systems (CPS): systems involving tight/complex coupling of computer and physical subsystems
Cyber Physical Systems (CPS): systems involving tight/complex coupling of computer and physical subsystems

Computer
Mechanics
Aerodynamics

Communications
Control

Material
Demand to use wireless links for safety and efficiency concerns.

The Operation Room Spider Web
Demand to use wireless links for safety and efficiency concerns.

The Operation Room Spider Web, after medical CPS safety interlocks
Demand to use wireless links for safety and efficiency concerns.

Spider Web OR vs. Wireless OR
How to guarantee PTE safety despite of arbitrary wireless link failures?

Leasing Design Pattern

Hybrid Automata Modeling: formally describe, analyze, and use the design pattern
General concept of Leasing Design Pattern for CPS

PTE guarantee

Supervisor

Initiator

Participant

Participant

Participant
General concept of Leasing Design Pattern for CPS
PTE guarantee
General concept of Leasing Design Pattern for CPS

PTE guarantee

Initiator

Supervisor

Request

Fallback

Participant

Participant
General concept of Leasing Design Pattern for CPS
PTE guarantee
General concept of Leasing Design Pattern for CPS
PTE guarantee

Supervisor

Request

Initiator

Fallback

Participant

Lease

Participant
General concept of Leasing Design Pattern for CPS
PTE guarantee

Initiator

Supervisor

Participant

Participant

Fallback

Request

Lease
General concept of Leasing Design Pattern for CPS

PTE guarantee

Supervisor

Initiator

Participant

Participant

Request

Lease

Lease
General concept of Leasing Design Pattern for CPS
PTE guarantee

- Initiator
- Supervisor
- Participant

Lease

Approve

Request

Initiator

Participant

Participant
General concept of Leasing Design Pattern for CPS

PTE guarantee
The same scenario can also apply to purely cyber systems. What's the difference that CPS makes?
CPS Features: 1. real-time matters; 2. real-time PTE even when aborting/canceling. (+ 3. arbitrary comm. failures)
Leasing Design Pattern for PTE Safety Rules:

Sketch of Supervisor's hybrid automaton.
Leasing Design Pattern for PTE Safety Rules: sketch of Initiator's hybrid automaton
Leasing Design Pattern for PTE Safety Rules: sketch of Participant's hybrid automaton

Intermediate Location btw two events. Cost 0 time.
Emulation Scheme

Supervisor: $T_{\text{fb,0}}^{\text{min}} = 13(s), T_{\text{wait}}^{\text{max}} = 3(s)$

Initiator: $T_{\text{req,2}}^{\text{max}} = 5(s), T_{\text{enter,2}}^{\text{max}} = 10(s), T_{\text{run,2}}^{\text{max}} = 20(s), T_{\text{exit,2}} = 1.5(s)$

Ventilator: $T_{\text{enter,1}}^{\text{max}} = 3(s), T_{\text{run,1}}^{\text{max}} = 35(s), T_{\text{exit,1}} = 6(s)$

PTE safeguard intervals: $T_{\text{risky:1\rightarrow2}}^{\text{min}} = 3(s), T_{\text{safe:2\rightarrow1}}^{\text{min}} = 1.5(s)$
Example Scenario

Supervisor

SpO₂ Sensor

Ventilator

Laser Scalpel

Surgeon

Patient
Example Scenario

Supervisor

Ventilator Pausing

Laser Scalpel

Surgeon

SpO₂ Sensor

Patient
Example Scenario

- Patient
- SpO₂ Sensor
- Supervisor
- Ventilator (Pausing)
- Surgeon
- Laser Scalpel

Diagram showing the interactions between the patient, SpO₂ sensor, supervisor, ventilator, surgeon, and laser scalpel.
Example Scenario

- Supervisor
- Patient
- SpO₂ Sensor
- Ventilator Pausing
- Laser Scalpel Shooting
- Surgeon
Example Scenario

- Patient
- SpO2 Sensor
- Supervisor
- Ventilator
  - Pausing
- Surgeon
  - Lost
- Laser Scalpel
Example Scenario

Supervisor

Patient

Ventilator

Pausing

Laser Scalpel

Surgeon

SpO₂ Sensor
Example Scenario

- **SpO₂ Sensor**
- **Ventilator**
- **Laser Scalpel**
- **Supervisor**
- **Surgeon**
- **Patient**
Example Scenario

- Supervisor
- Ventilator Pausing
- Laser Scalpel
- Surgeon
- SpO₂ Sensor
- Patient
Example Scenario

Supervisor

SpO₂ Sensor

Ventilator Pausing

Laser Scalpel

Surgeon

Patient
Example Scenario

- Patient
- SpO2 Sensor
- Supervisor
- Ventilator
- Pausing
- Surgeon
- Laser Scalpel

Diagram shows the interactions between the patient, SpO2 sensor, supervisor, ventilator, and surgeon with the laser scalpel.
Example Scenario

- Patient
- SpO2 Sensor
- Supervisor
- Ventilator
- Pausing
- Laser Scalpel
- Surgeon
- lost
Example Scenario

- Supervisor
- SpO₂ Sensor
- Patient
- Ventilator
- Pausing Laser
- Surgeon
- Scalpel
Example Scenario

Supervisor

Ventilator

SpO2 Sensor

Surgeon

Patient

Laser Scalpel
Example Scenario

Supervisor

SpO₂ Sensor

Ventilator

Patient

Surgeon

Laser Scalpel