Guaranteeing Proper-Temporal-Embedding Safety Rules in Wireless CPS: A Hybrid Formal Modeling Approach

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

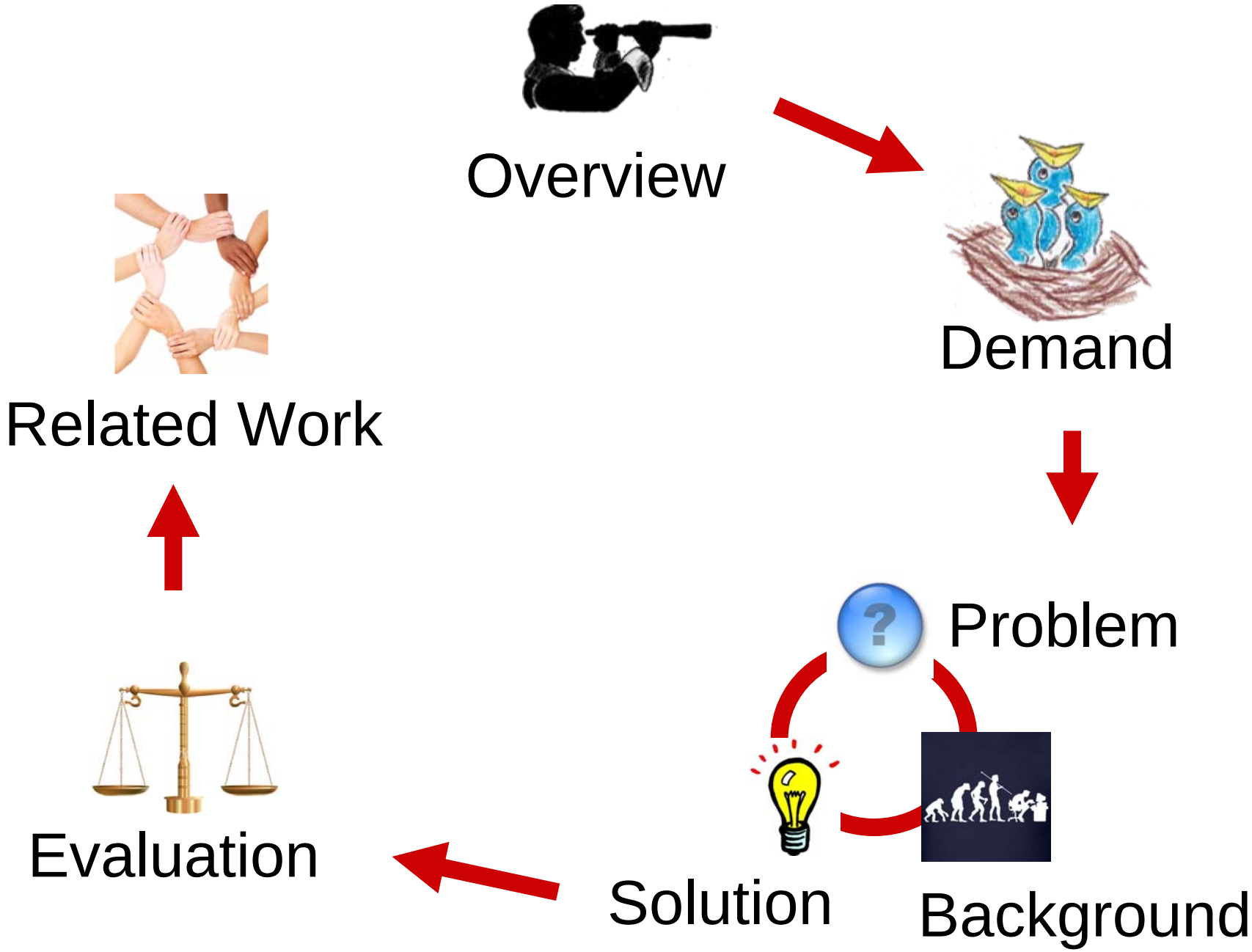
[*] Embedded Systems & Networking Lab, Dept. of Computing, **The Hong Kong Polytechnic Univ.**

[†] 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


Overview
Demand
Problem
Background
Solution
Evaluation
Related Work

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

Life/Mission critical CPS demand wireless

Wireless is unreliable

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

Life/Mission critical CPS demand wireless

PTE Safety Guarantee

Wireless is unreliable

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

Life/Mission critical CPS demand wireless

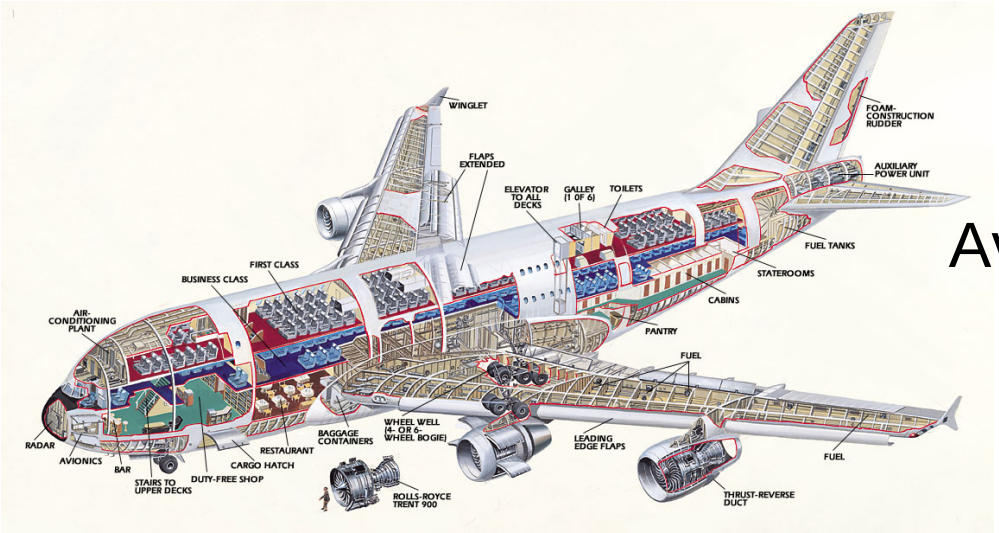
Conflict

Design Pattern
Hybrid Modeling

PTE Safety Guarantee

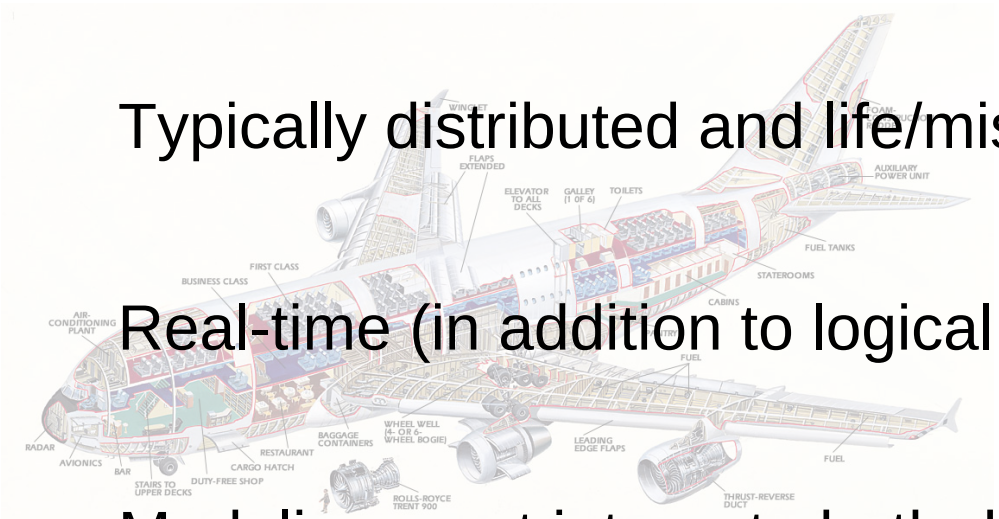
Wireless is unreliable

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



Avionics

CPS Features



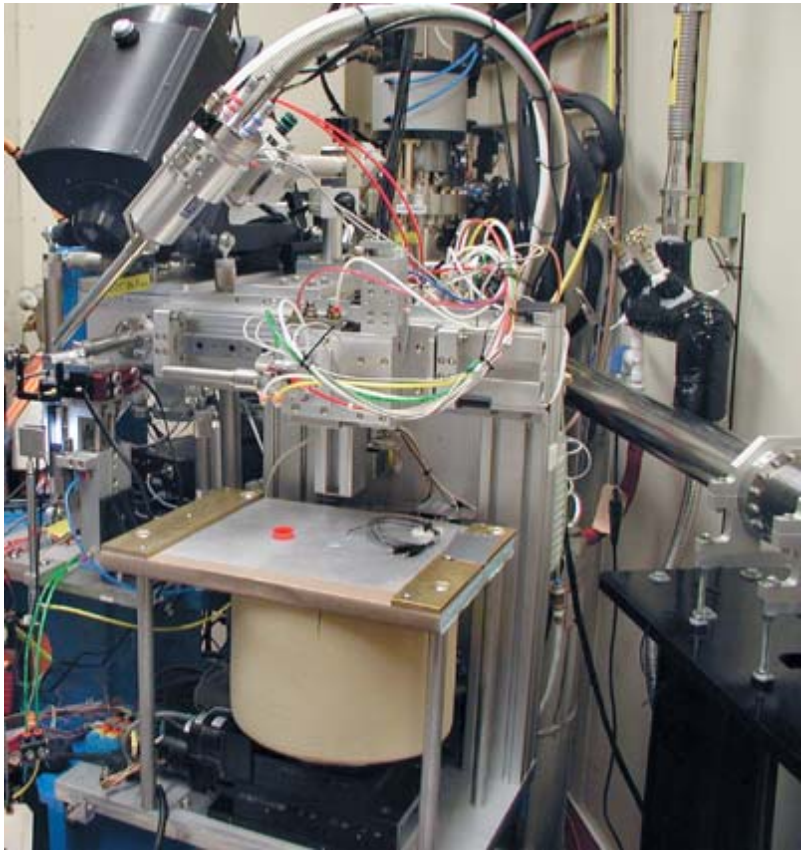
Typically distributed and life/mission-critical

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

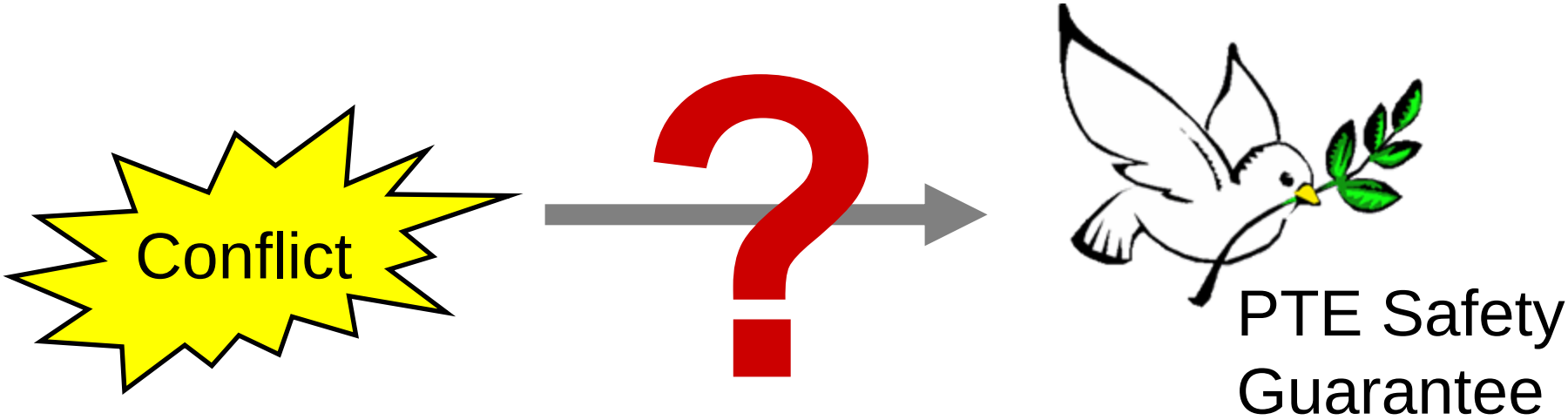
How to guarantee the safety of life/mission critical wireless CPS?

Life/Mission critical CPS demand wireless

Wireless is unreliable

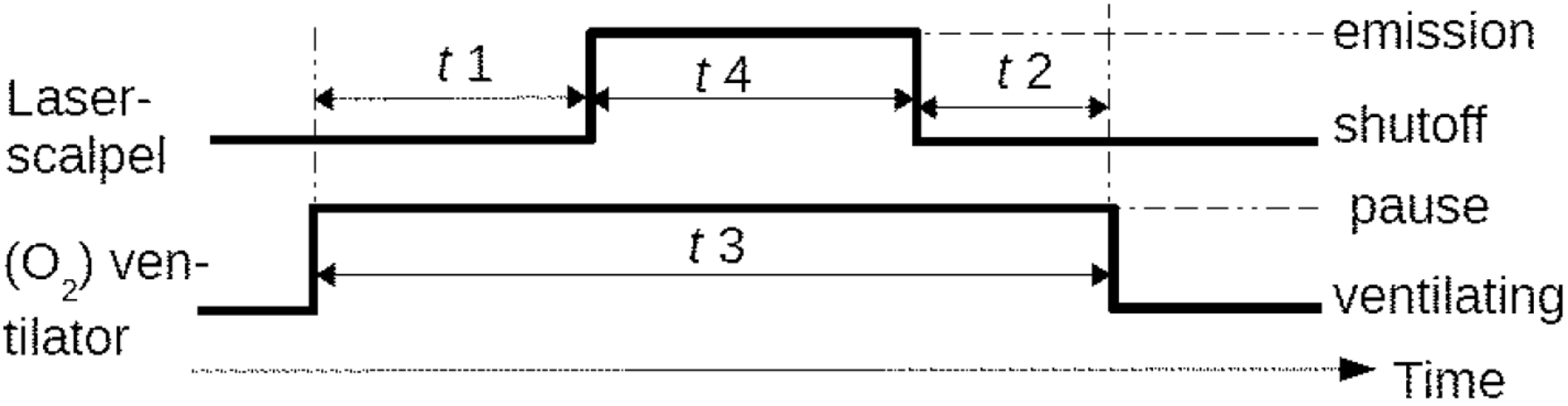
How to guarantee the Proper-Temporal-Embedding (PTE) safety rule of life/mission critical wireless CPS?

Life/Mission critical CPS demand wireless

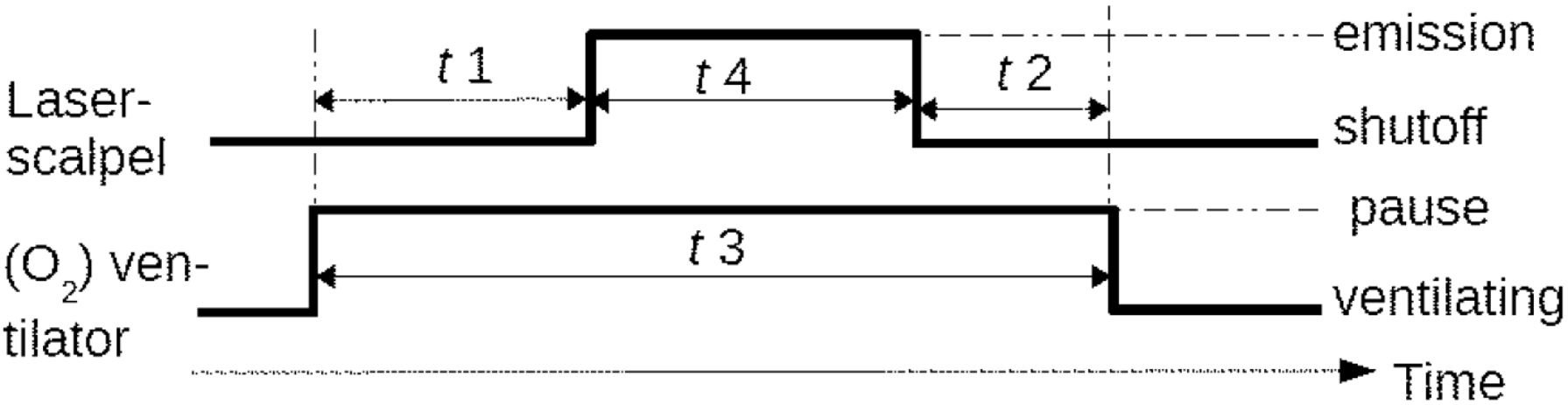


Wireless is unreliable

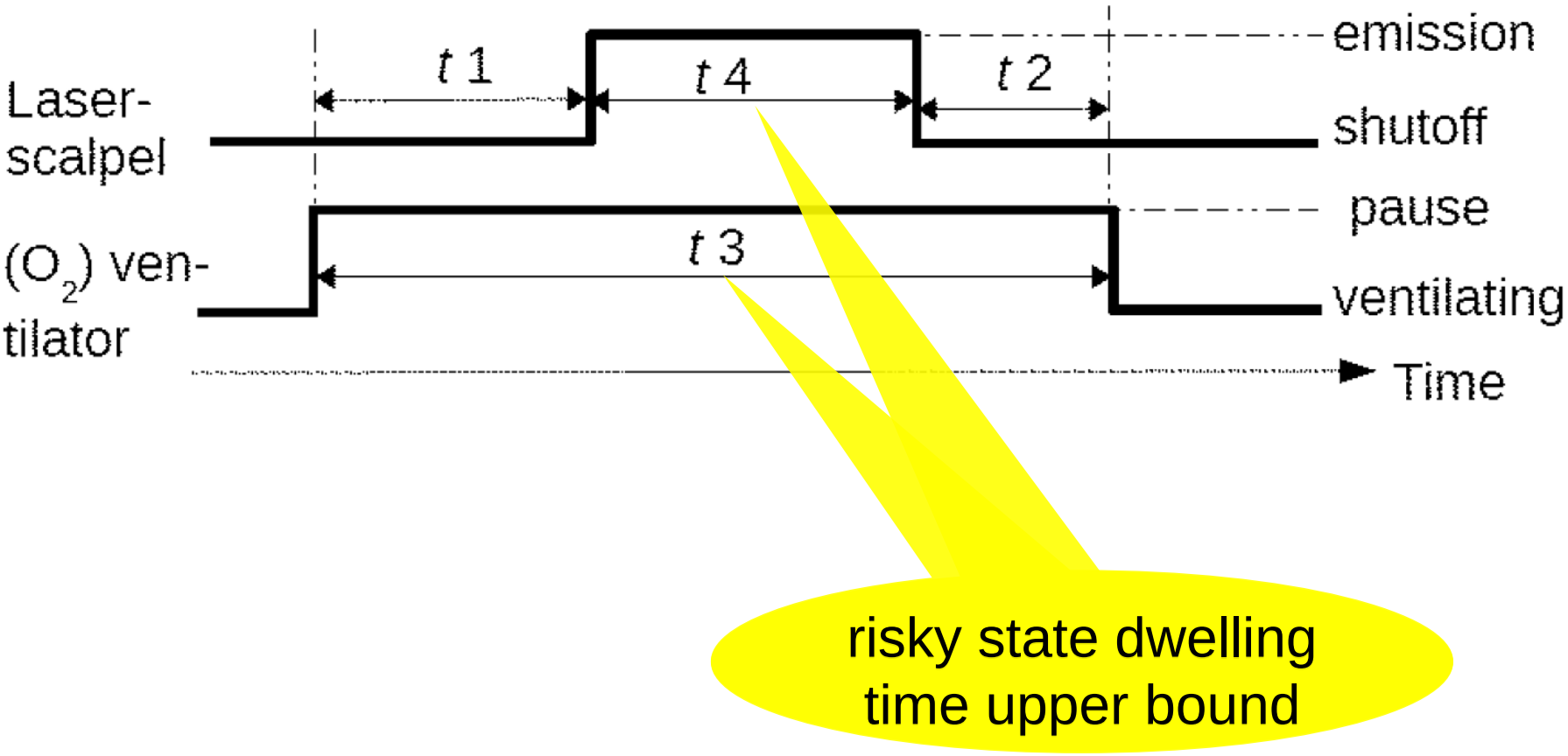
What is Proper-Temporal-Embedding (PTE) safety rule?



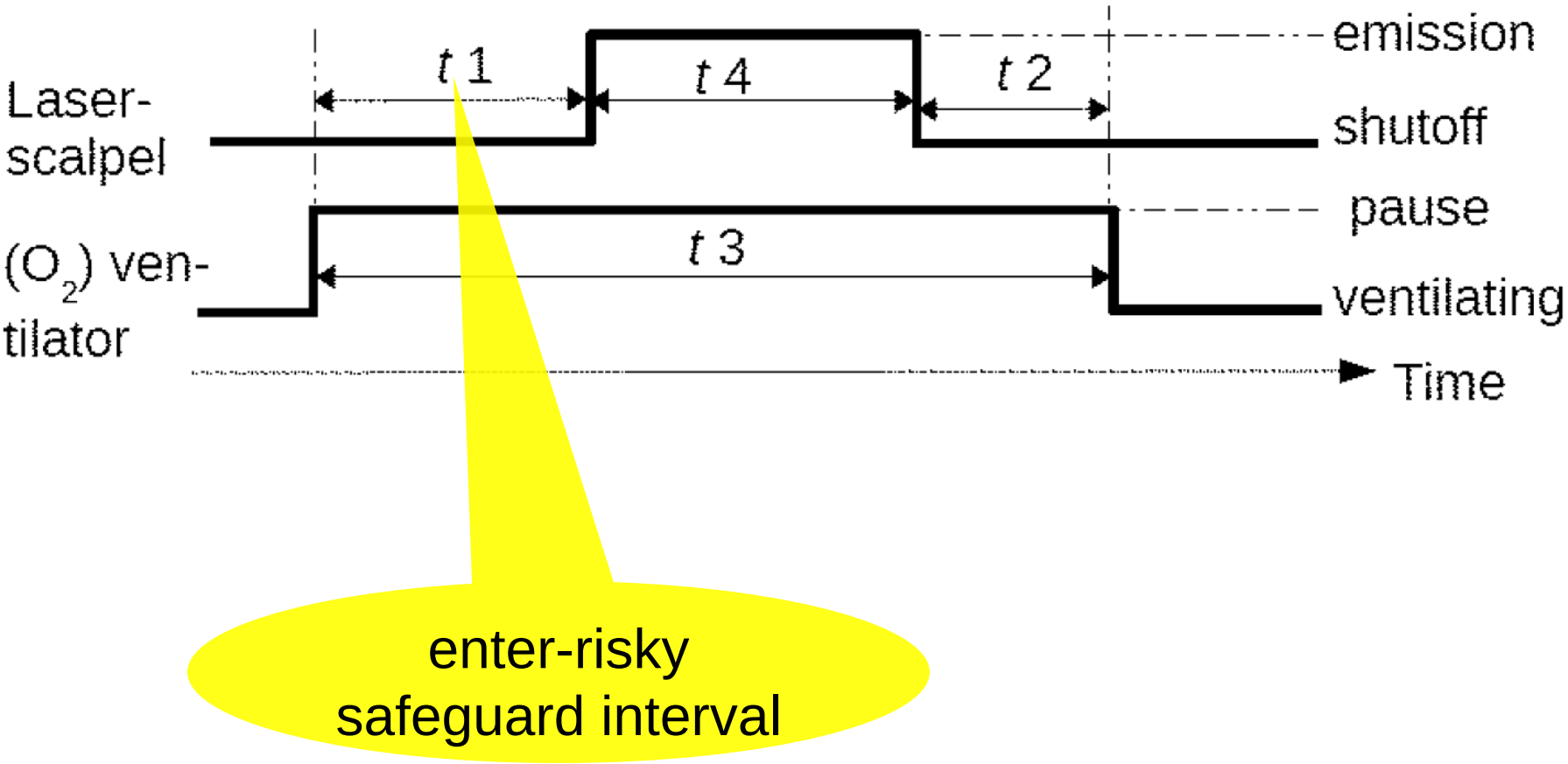
CPS Feature 2: real-time (in addition to logical time) matters!



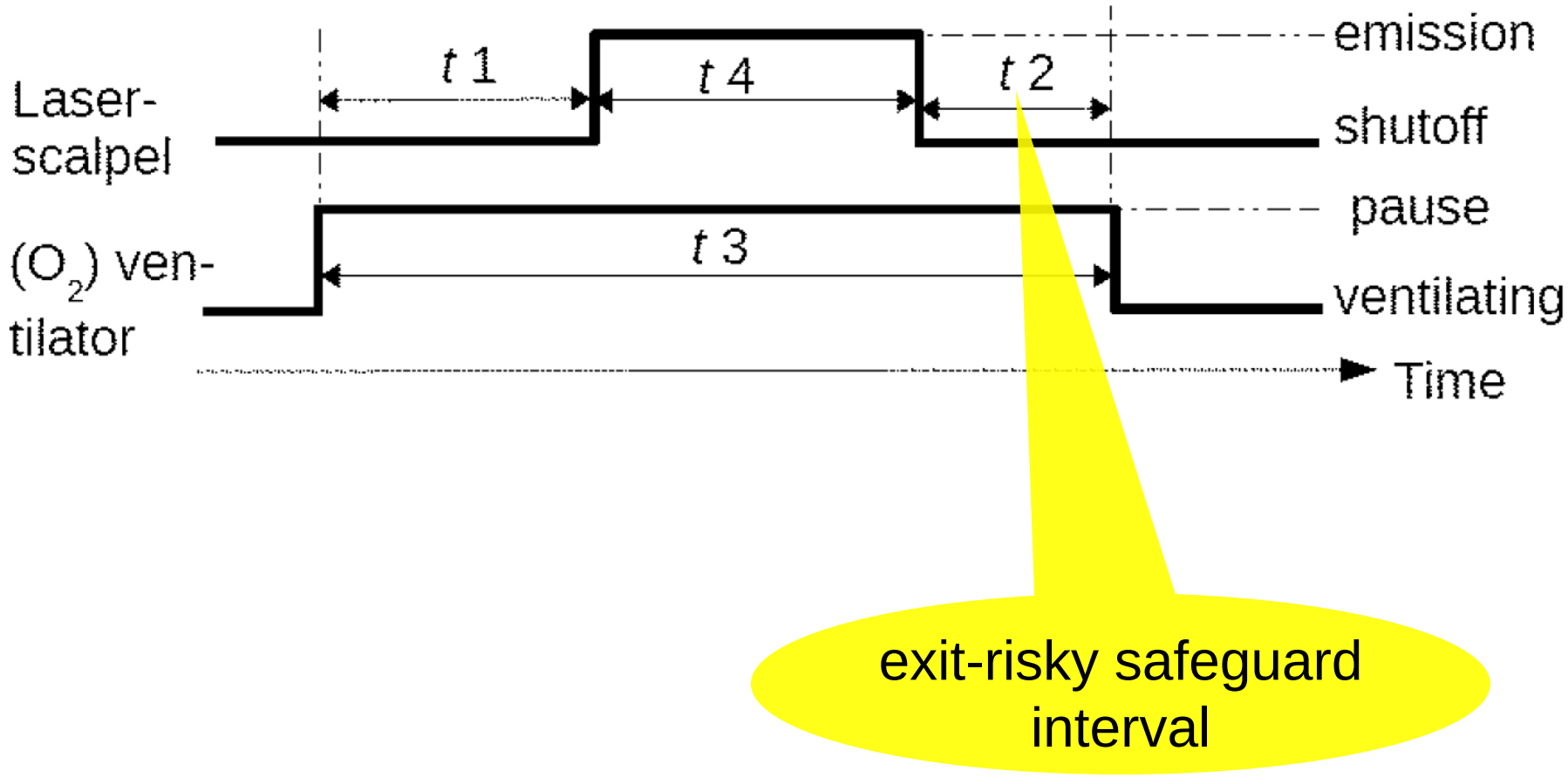
CPS Feature 2: real-time (in addition to logical time) matters!



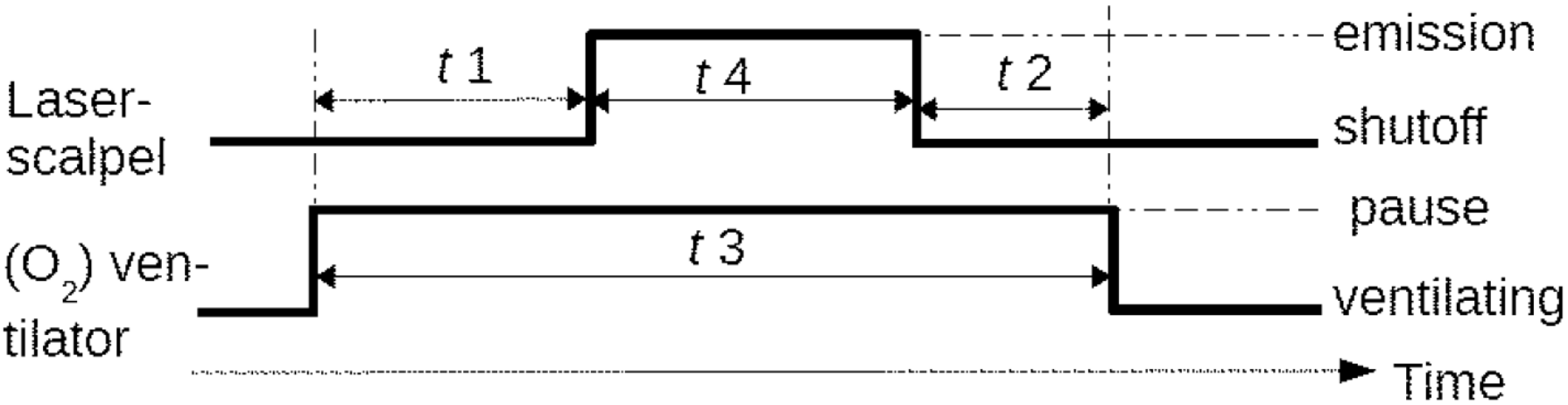
CPS Feature 2: real-time (in addition to logical time) matters!



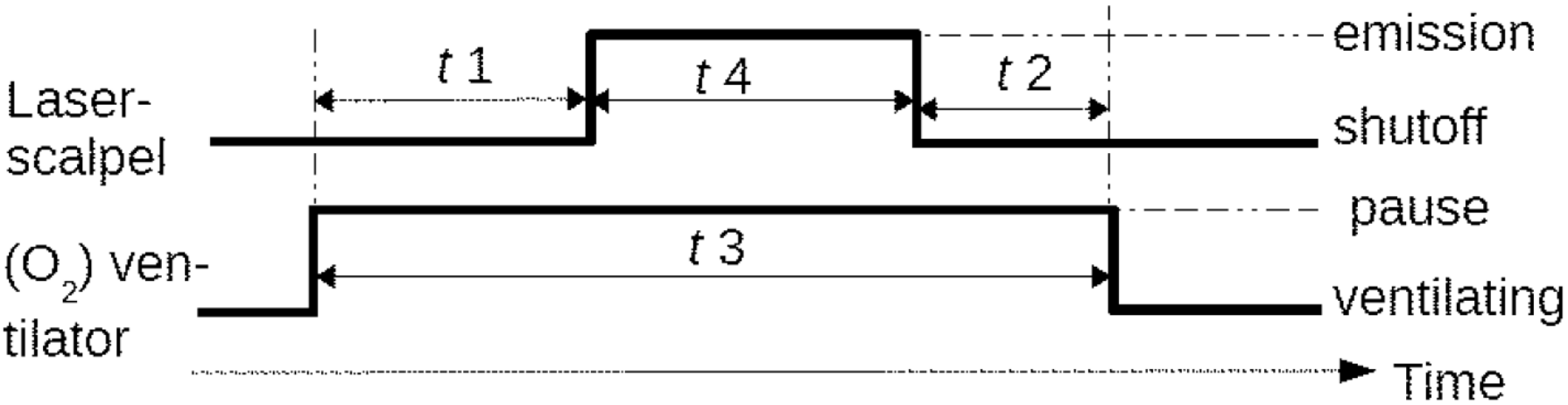
CPS Feature 2: real-time (in addition to logical time) matters!



How to guarantee PTE safety despite of arbitrary wireless link failures?

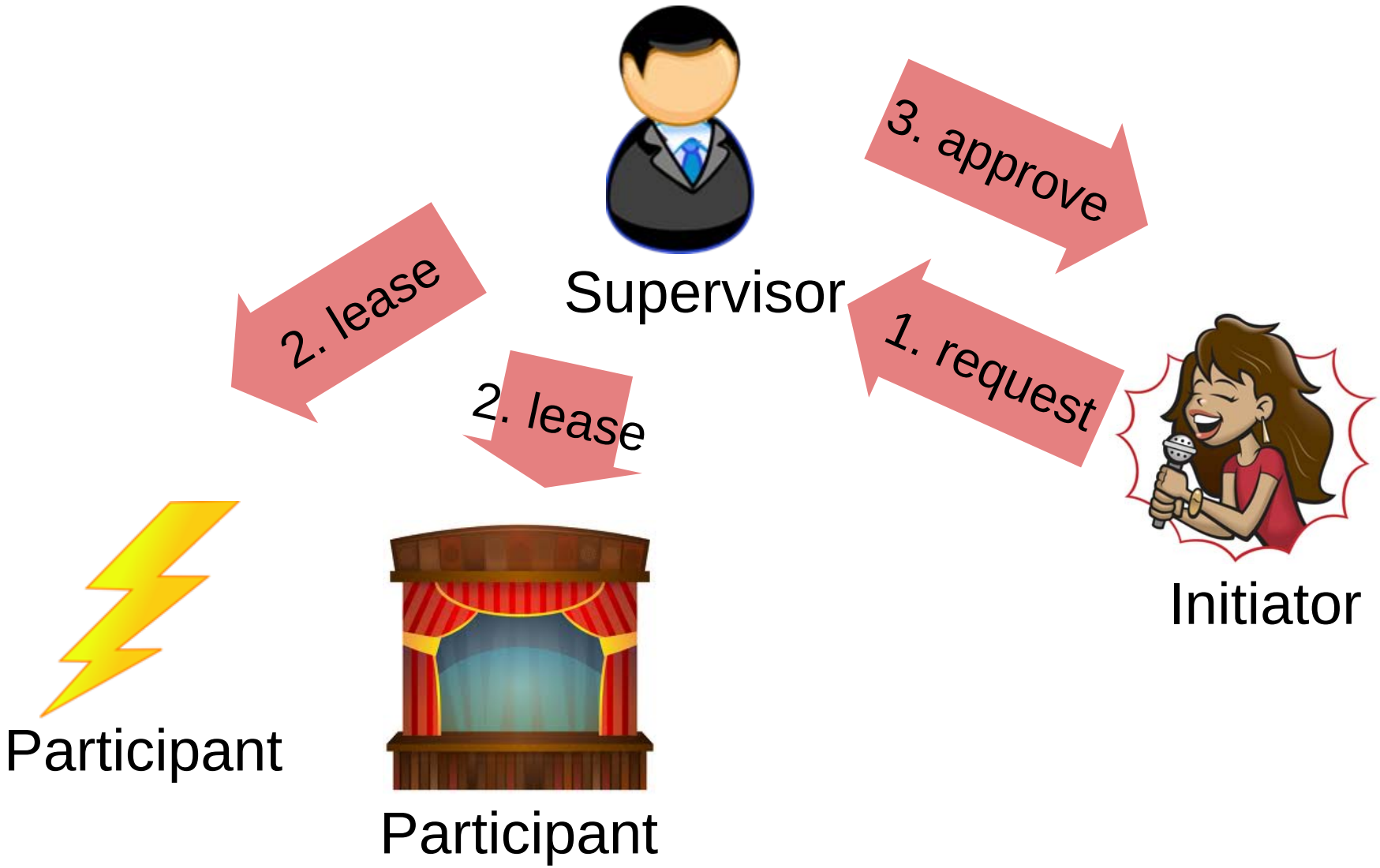


How to guarantee PTE safety despite of arbitrary wireless link failures?

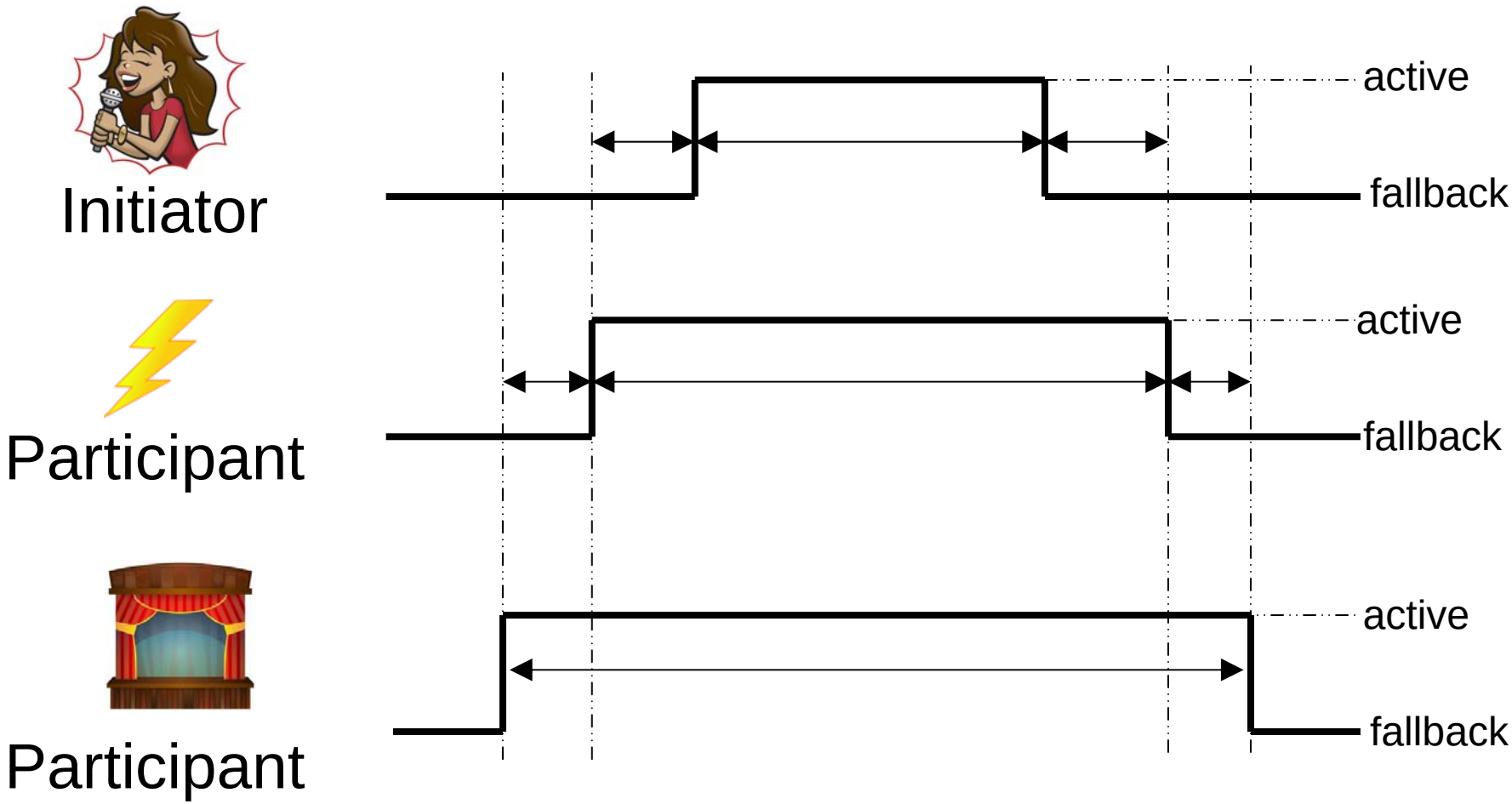


Leasing Design Pattern:
risky state dwelling time must be leased.

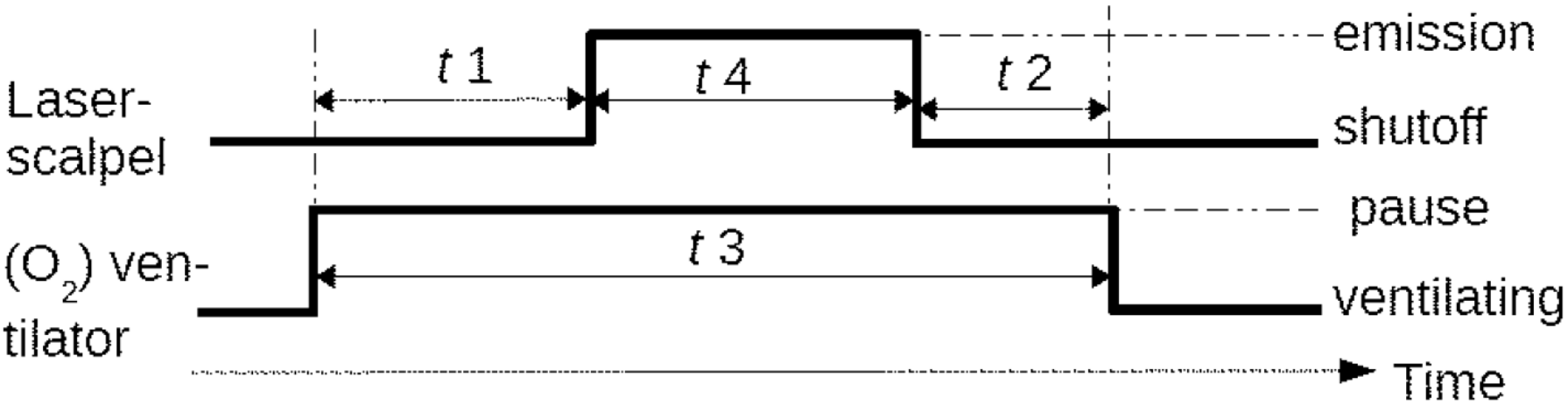
General concepts of Leasing design pattern: each CPS entity takes one of the 3 roles.



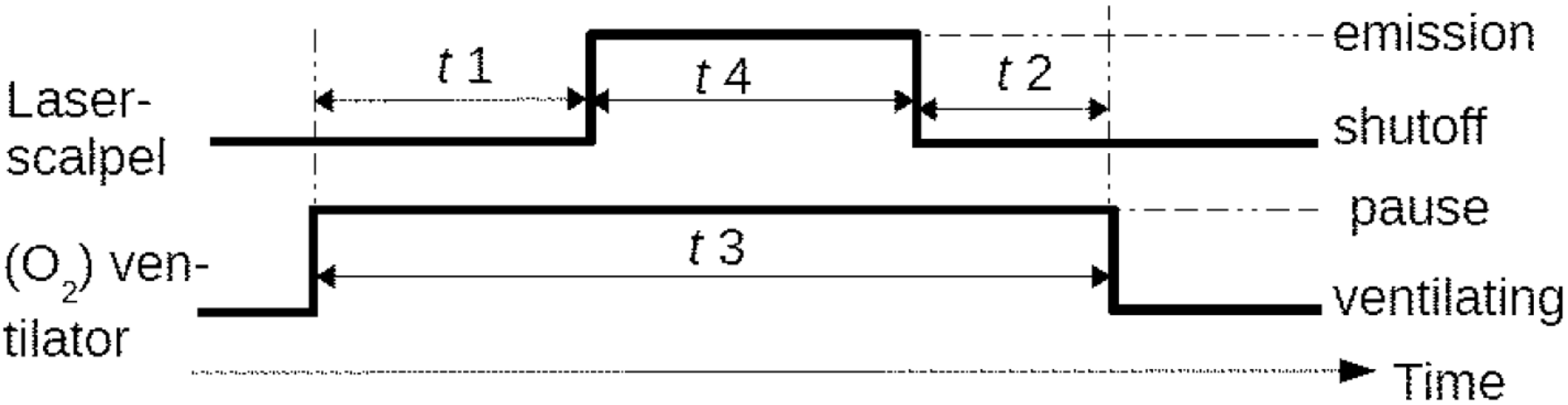
CPS Features: 1. real-time matters; 2. real-time PTE even when aborting/canceling. (+ 3. arbitrary comm. failures)



How to formally describe, analyze, and use Leasing design pattern in the context of CPS?



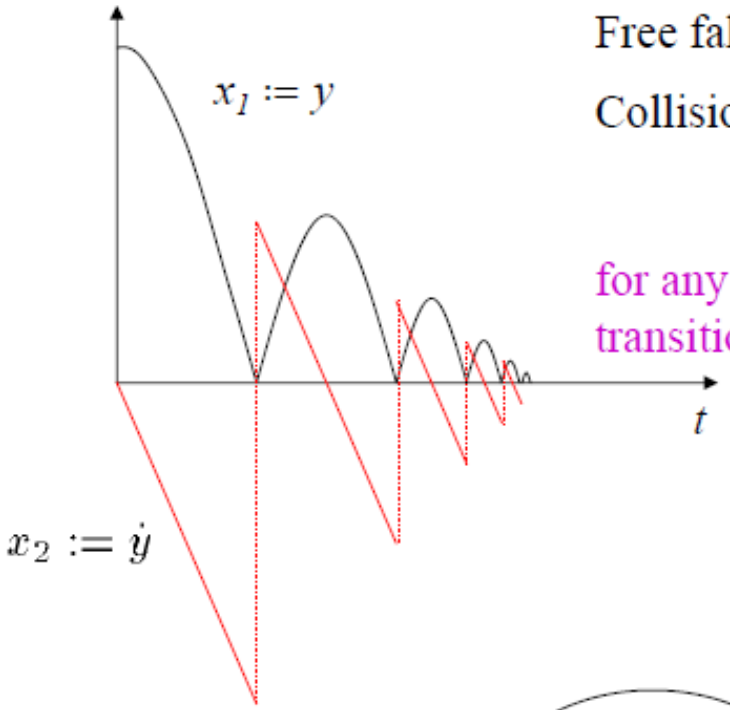
How to formally describe, analyze, and use Leasing design pattern in the context of CPS?



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 $\equiv$ $\ddot{y} = -g$

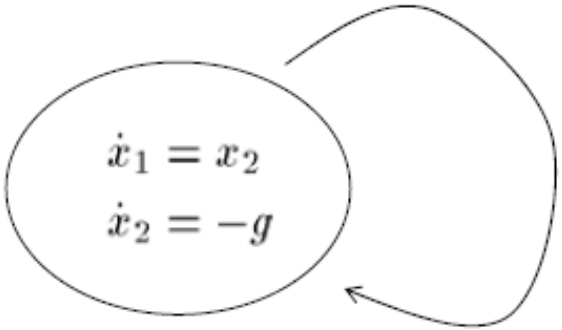
Collision $\equiv$ $y^+(t) = y^-(t) = 0$

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

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

guard or jump condition

$x_1 = 0$ & $x_2 < 0$?

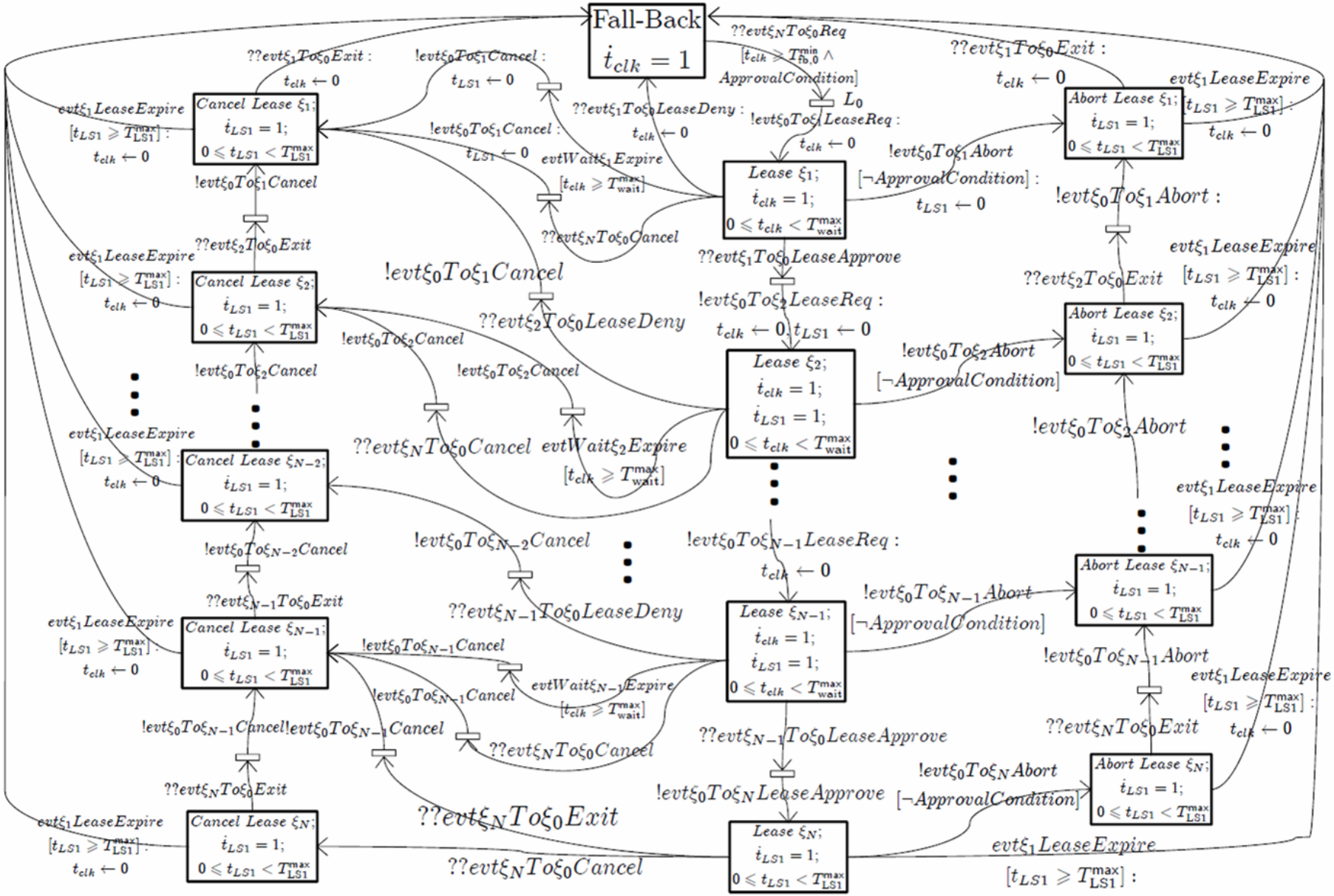


transition

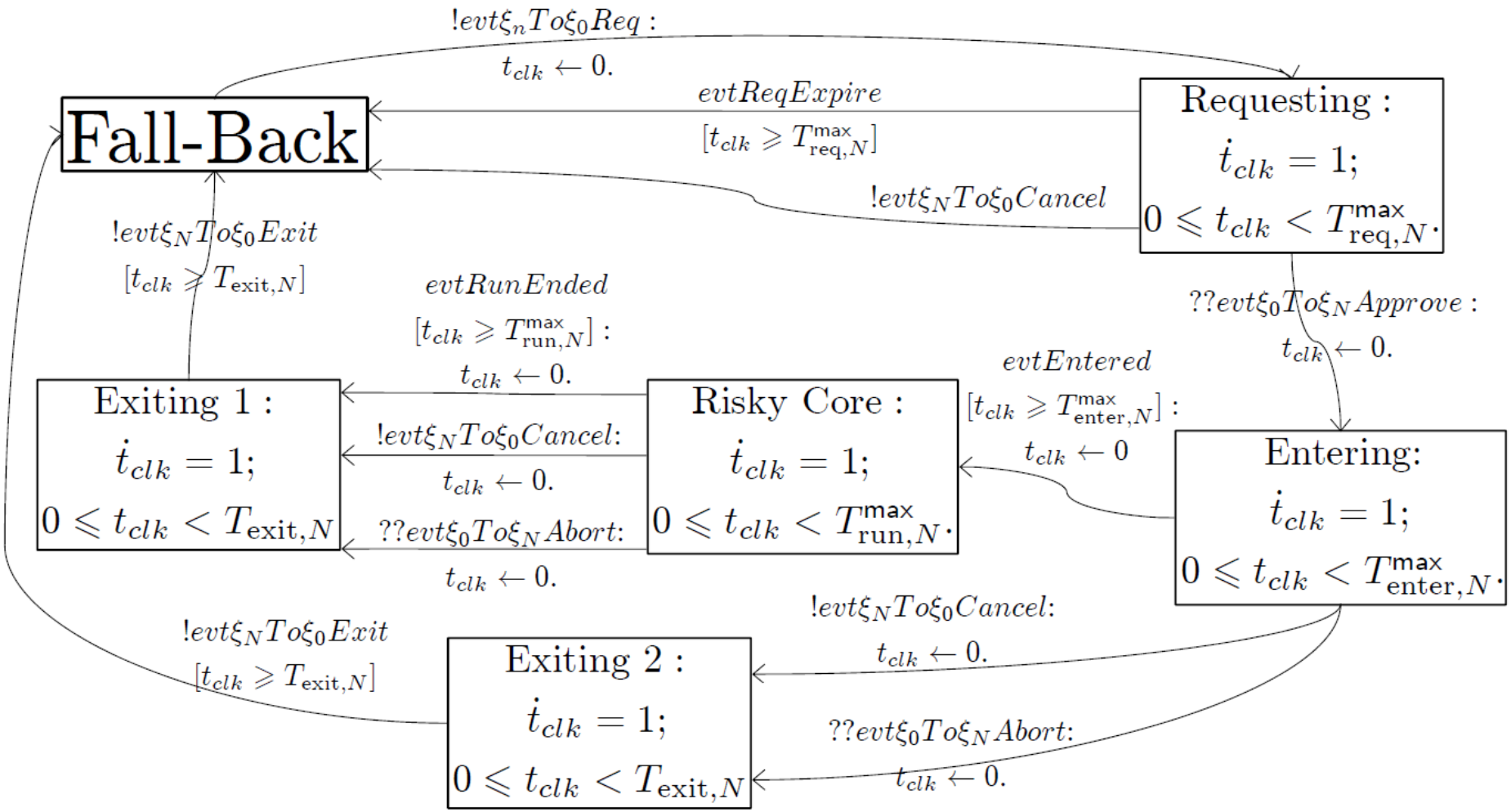
$x_2 := -c\,x_2^-$

state reset

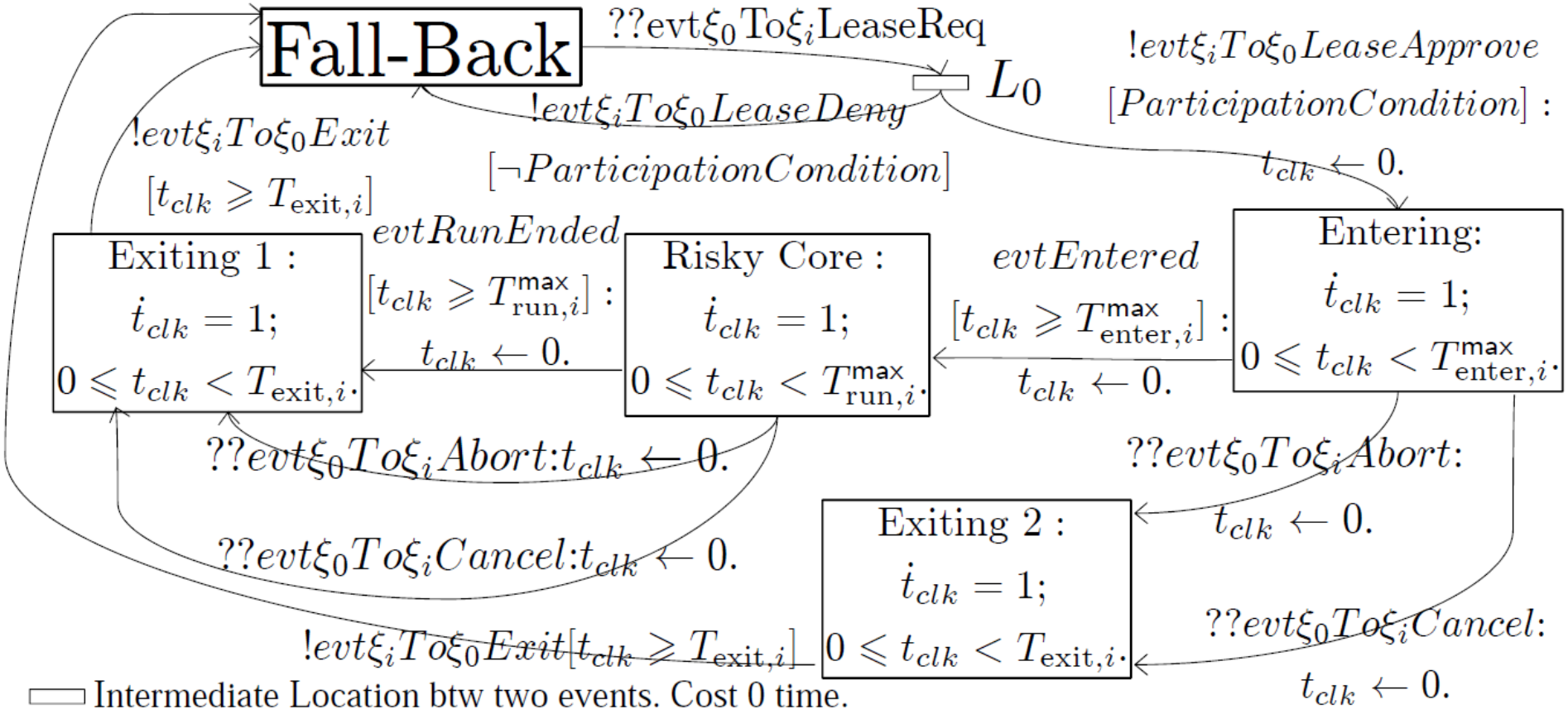
Leasing Design Pattern for PTE Safety Rules: detailed Supervisor's hybrid automaton



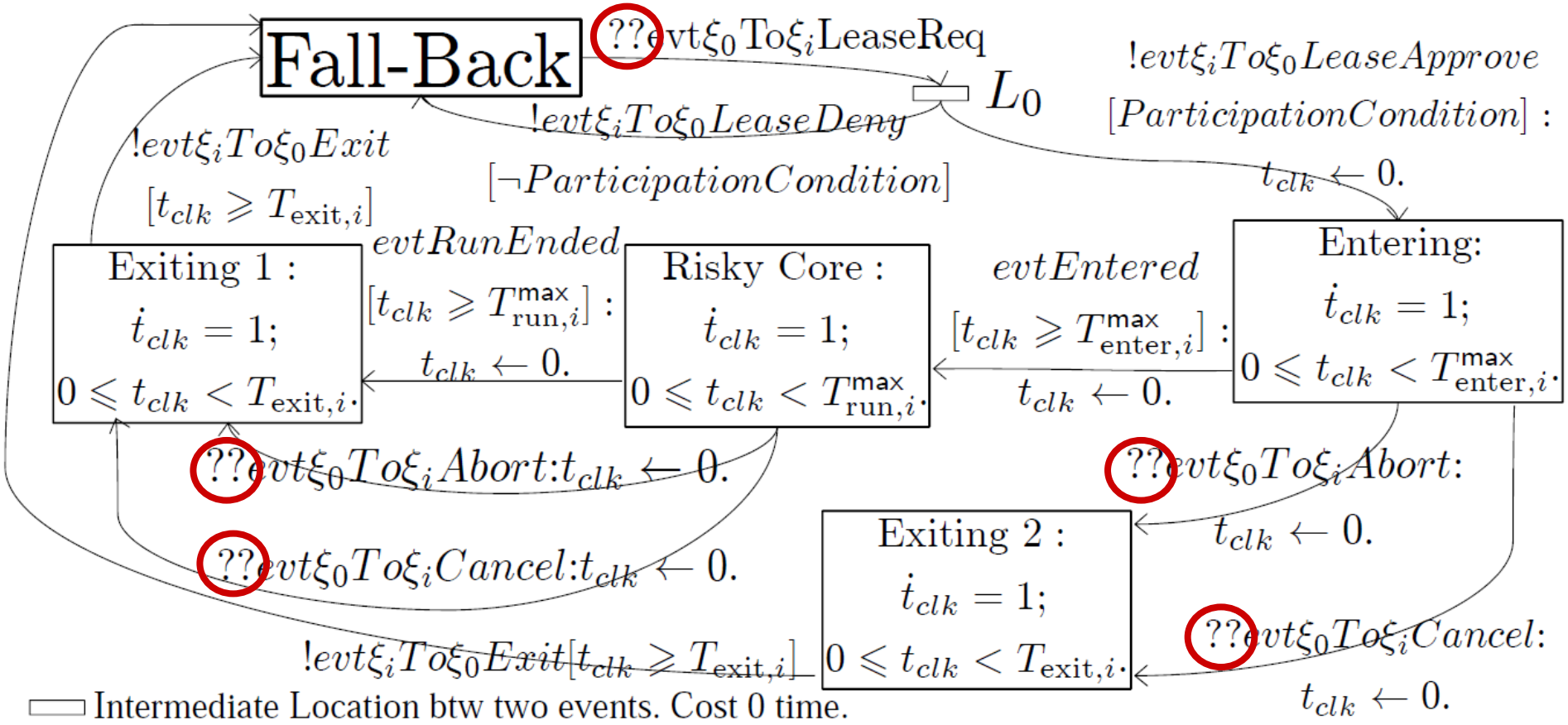
Leasing Design Pattern for PTE Safety Rules: detailed Initiator's hybrid automaton



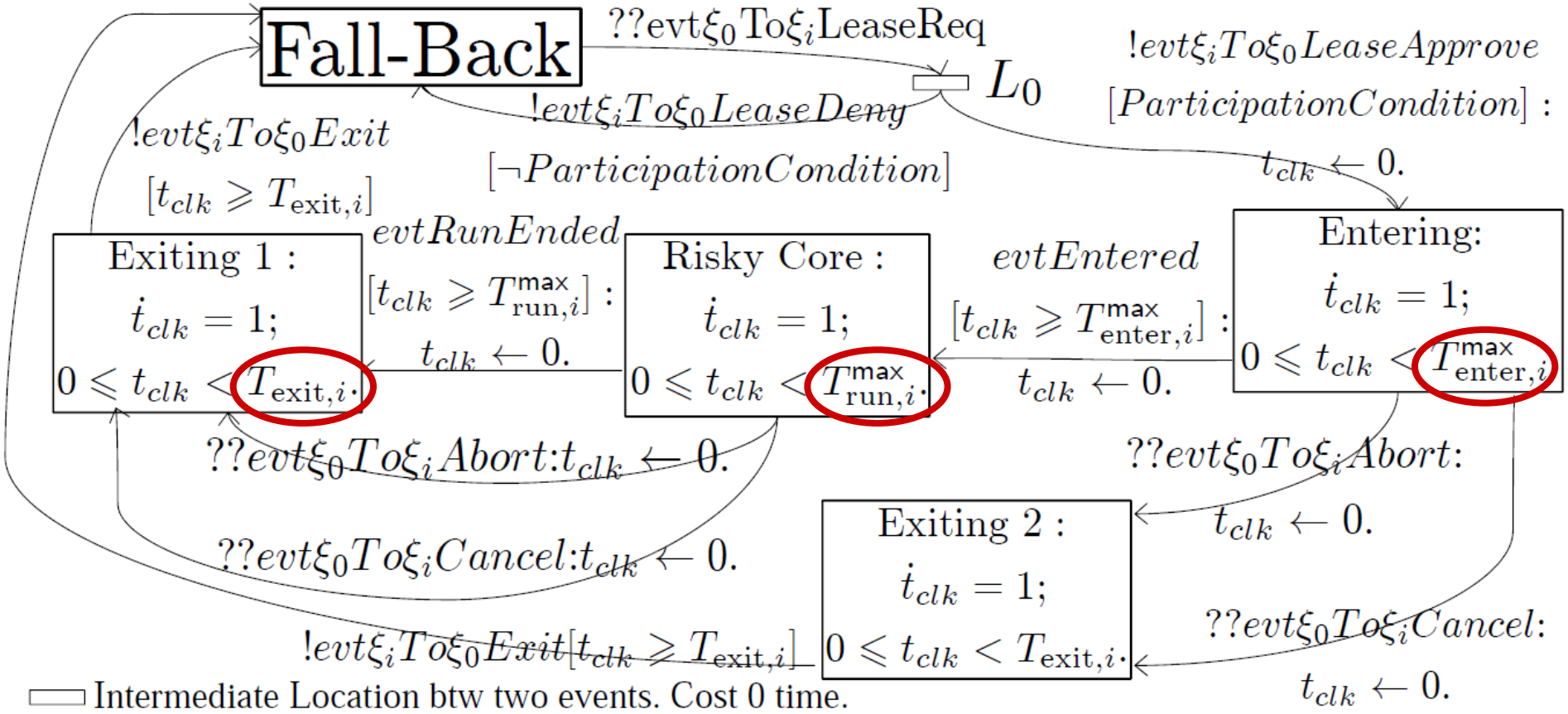
Leasing Design Pattern for PTE Safety Rules: detailed Participant's hybrid automaton



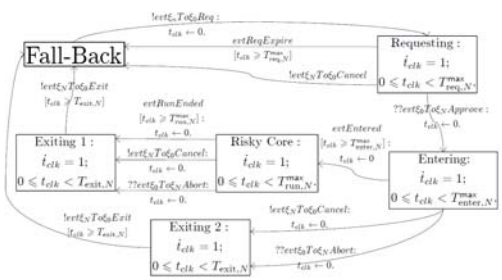
Leasing Design Pattern for PTE Safety Rules: detailed Participant's hybrid automaton

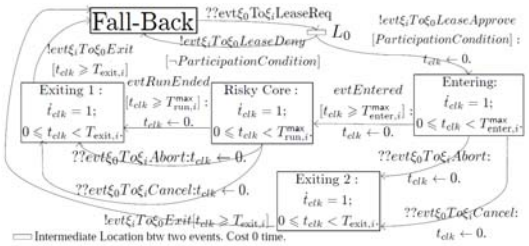


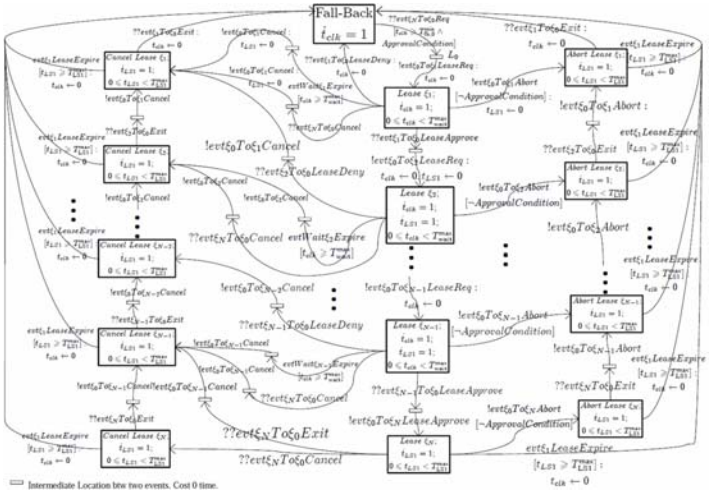
Leasing Design Pattern for PTE Safety Rules: detailed Participant's hybrid automaton



Validity of the design pattern







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 ($T^{\mathsf{max}}_{\text{wait}}$, $T^{\mathsf{min}}_{\text{fb},0}$, $T^{\mathsf{max}}_{\text{LS1}}$, $T^{\mathsf{max}}_{\text{req},N}$, $T^{\mathsf{max}}_{\text{enter},i}$, $T^{\mathsf{max}}_{\text{run},i}$, $T_{\text{exit},i}$, where $i = 1 \sim N$) are positive.

c2. $T^{\mathsf{max}}_{\text{LS1}} \stackrel{\mathsf{def}}{=} T^{\mathsf{max}}_{\text{enter},1} + T^{\mathsf{max}}_{\text{run},1} + T_{\text{exit},1} > NT^{\mathsf{max}}_{\text{wait}}$.

c3. $(N-1)T^{\mathsf{max}}_{\text{wait}} < T^{\mathsf{max}}_{\text{req},N} < T^{\mathsf{max}}_{\text{LS1}}$.

c4. $\forall i \in \{1, 2, \ldots, N\}$, there is

$$(i-1)T^{\mathsf{max}}_{\text{wait}} + T^{\mathsf{max}}_{\text{enter},i} + T^{\mathsf{max}}_{\text{run},i} + T_{\text{exit},i} \leq T^{\mathsf{max}}_{\text{LS1}}.$$

c5. $\forall i \in \{1, 2, \ldots, N-1\}$, there is

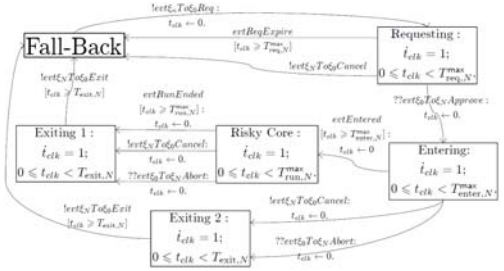
$$T^{\mathsf{max}}_{\text{enter},i} + T^{\mathsf{min}}_{\text{risky}:i \to i+1} < T^{\mathsf{max}}_{\text{enter},i+1}.$$

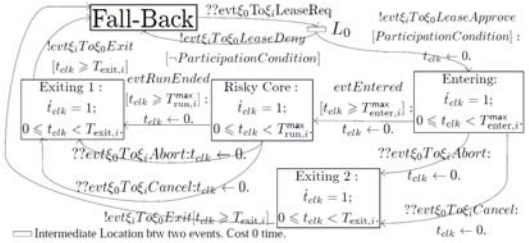
c6. $\forall i \in \{1, 2, \ldots, N-1\}$, there is

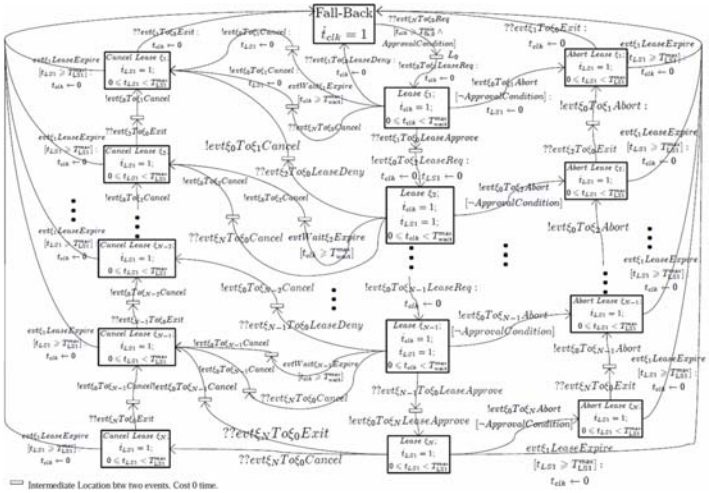
$$T^{\mathsf{max}}_{\text{enter},i} + T^{\mathsf{max}}_{\text{run},i} > T^{\mathsf{max}}_{\text{wait}} + T^{\mathsf{max}}_{\text{enter},i+1} + T^{\mathsf{max}}_{\text{run},i+1} + T_{\text{exit},i+1}.$$

c7. $\forall i \in \{1, 2, \ldots, N-1\}$, there is $T_{\text{exit},i} > T^{\mathsf{min}}_{\text{safe}:i+1 \to i}$.

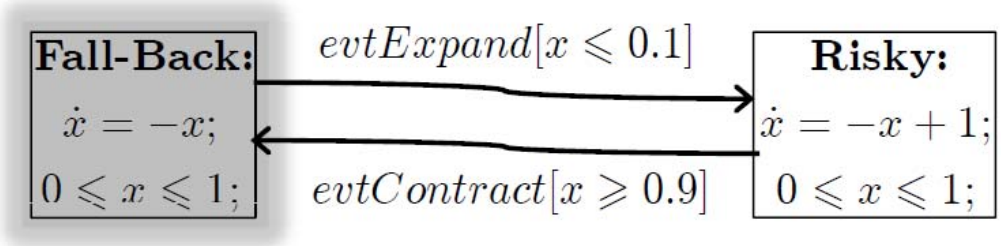
Using the design pattern: how to turn design pattern into detailed CPS designs?



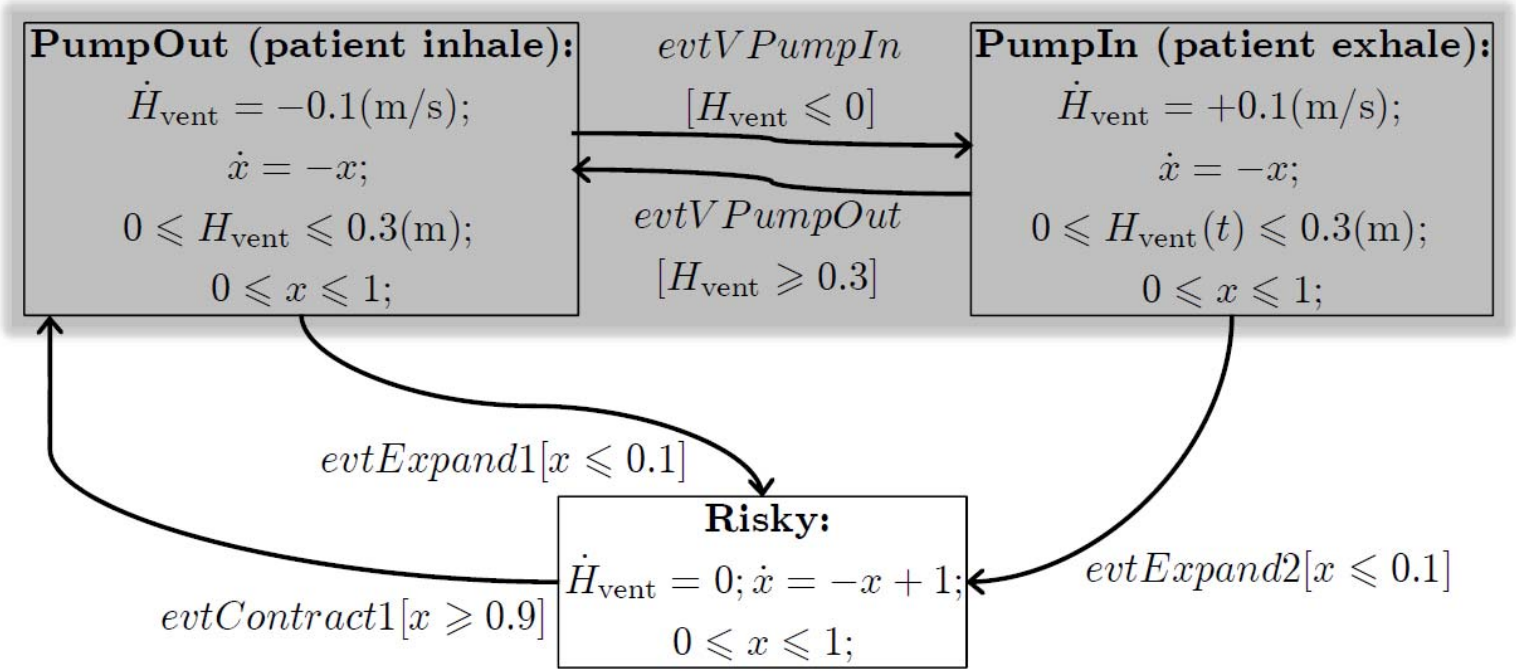




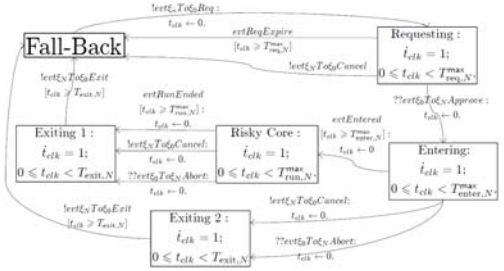
We proposed a formal procedure to elaborate a design pattern hybrid automaton into a detailed design hybrid automaton.

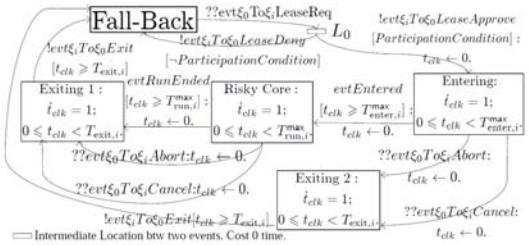


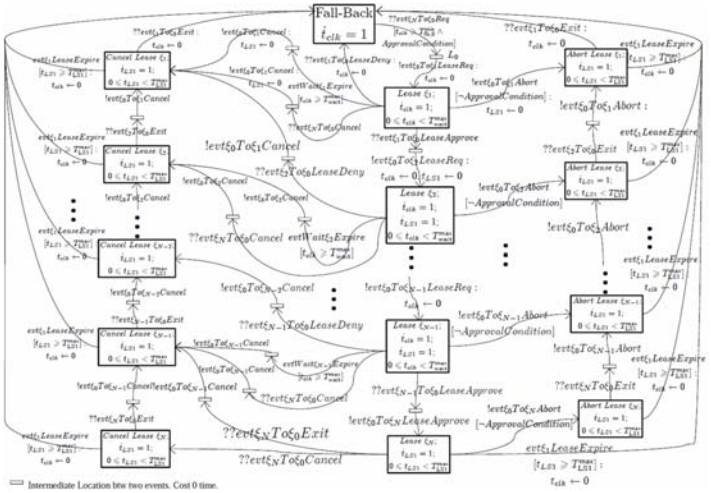
Elaborate



Validity of elaboration







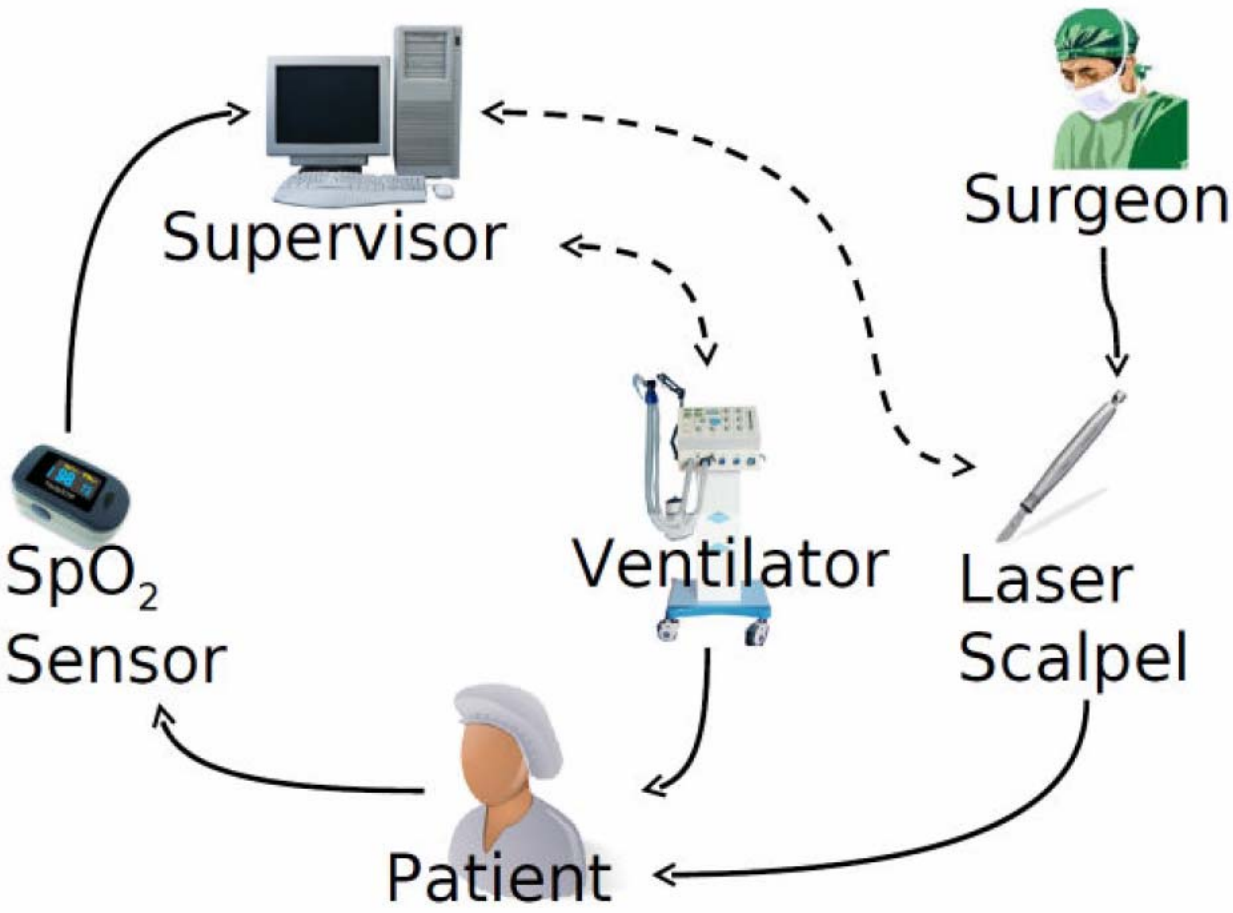
Theorem 2: If detailed design hybrid automata are respectively derived by elaborating corresponding design pattern hybrid automata, then PTE safety is guaranteed despite of arbitrary communications link failures.

Laser Tracheotomy Medical CPS: interconnect/interlock smart medical devices to increase safety

Laser Tracheotomy without Device Interlock

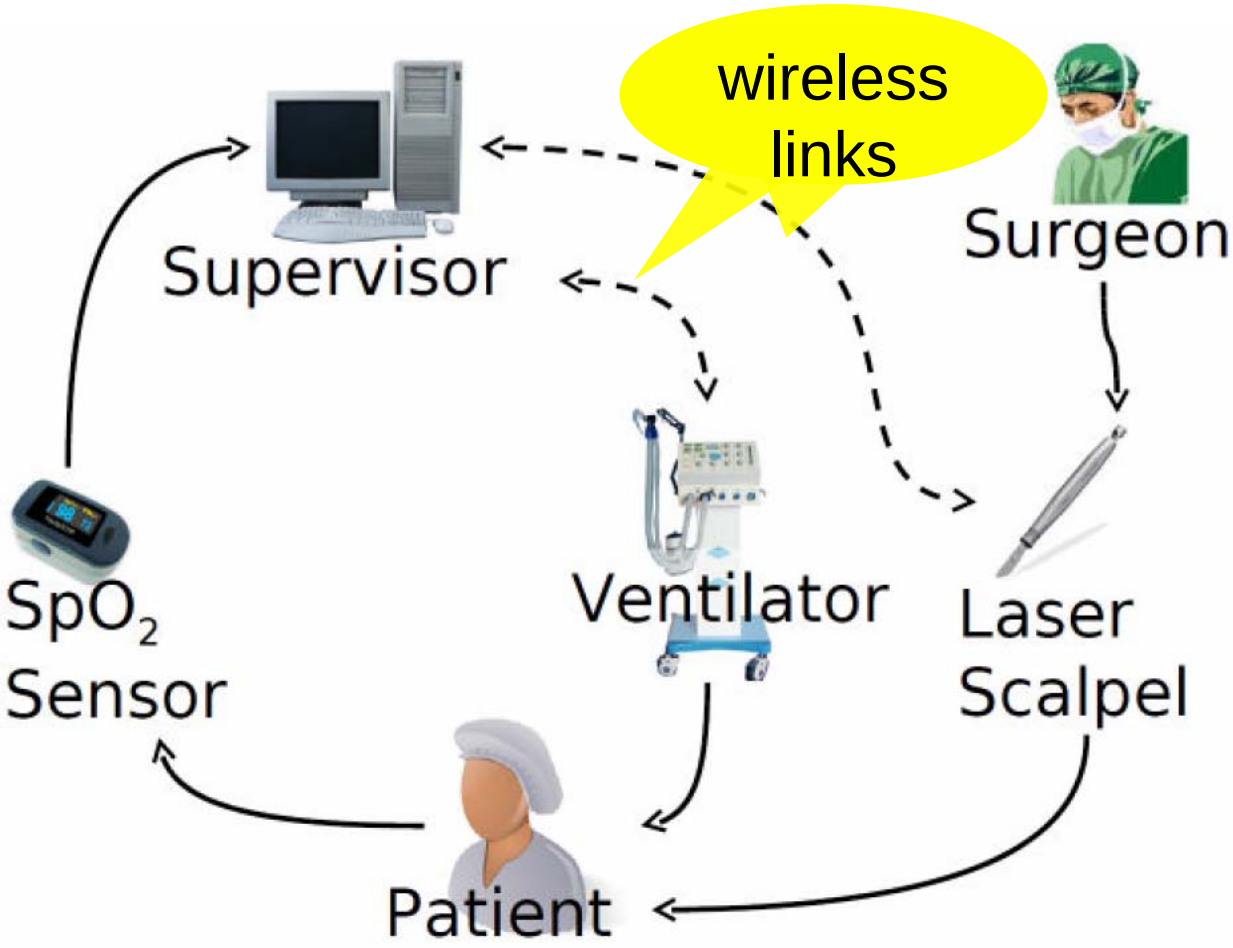
Laser Tracheotomy Medical CPS: interconnect/interlock smart medical devices to increase safety

Laser Tracheotomy CPS

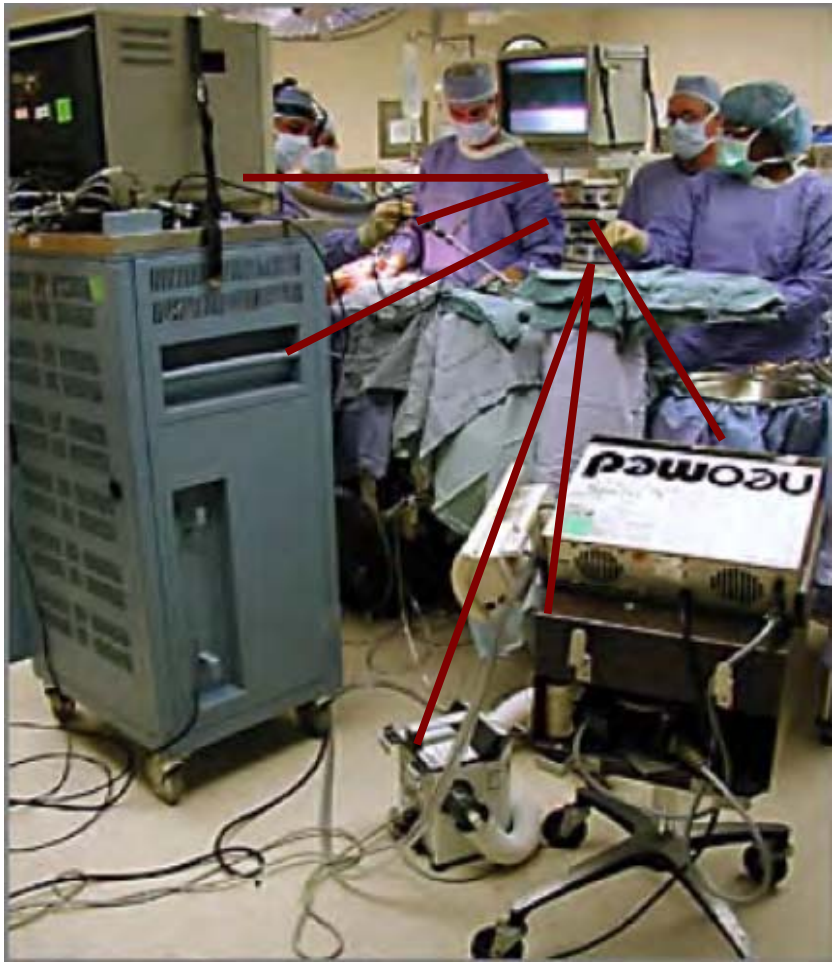


Demand to use wireless links for safety and efficiency concerns.

Laser Tracheotomy CPS

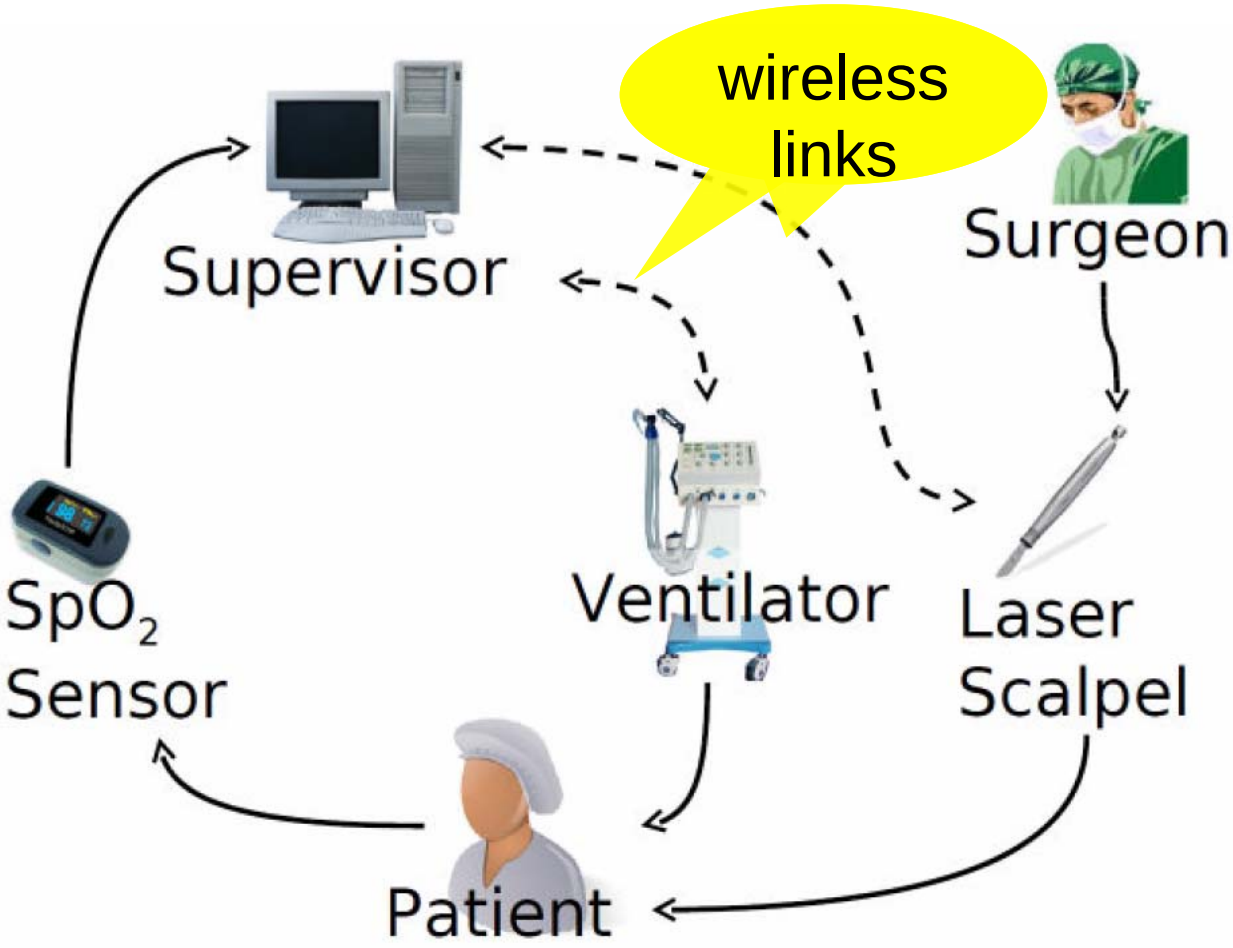


Demand to use wireless links for safety and efficiency concerns.

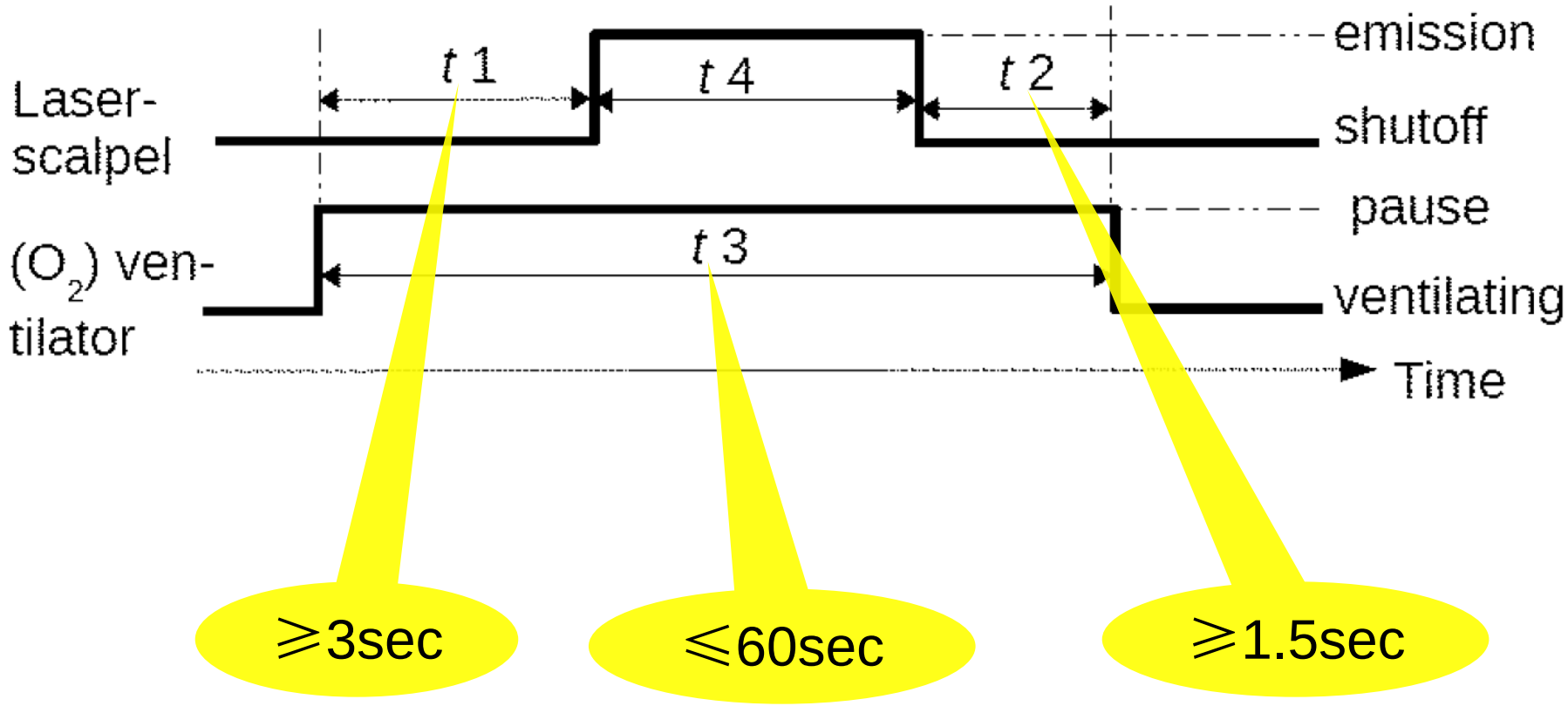


Demand to use wireless links for safety and efficiency concerns.

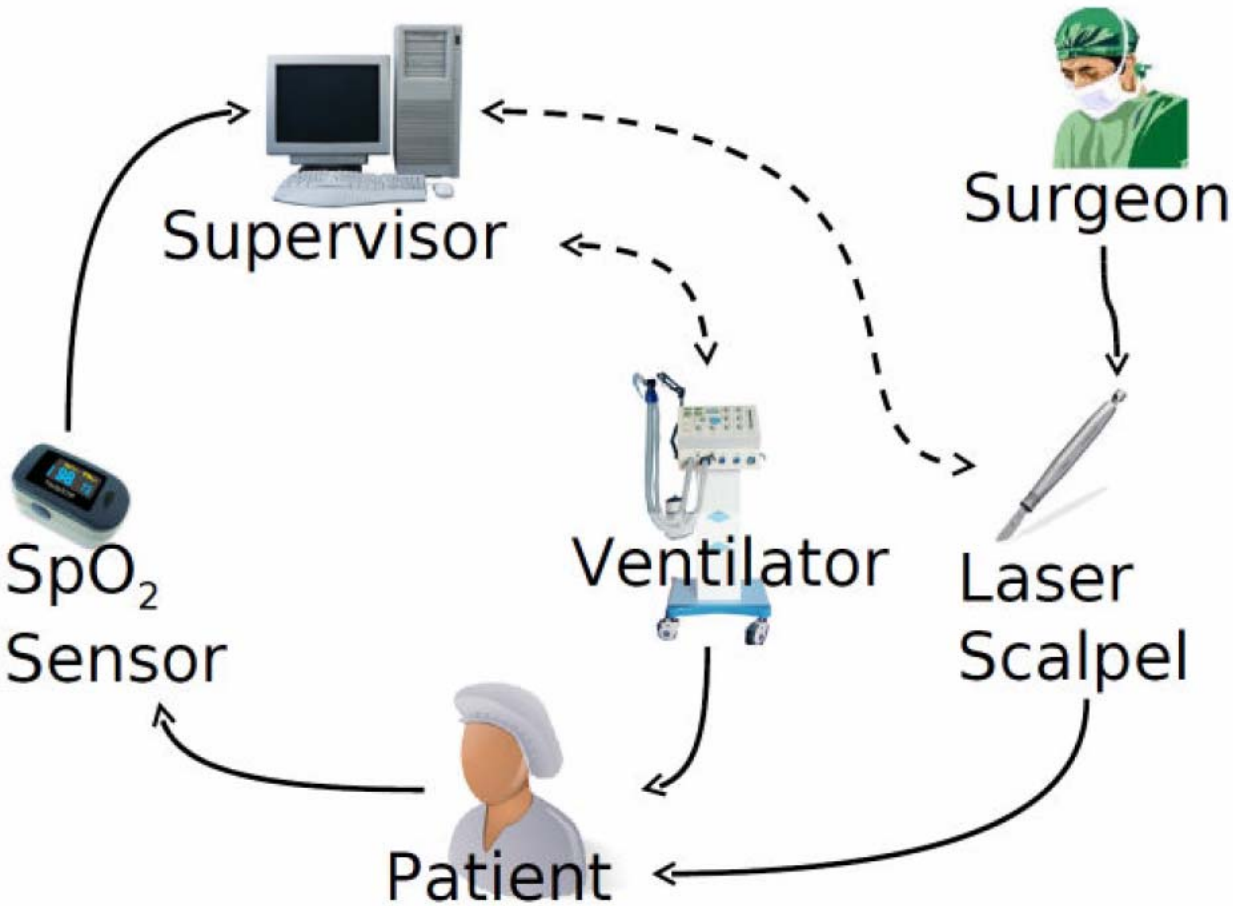
Laser Tracheotomy CPS



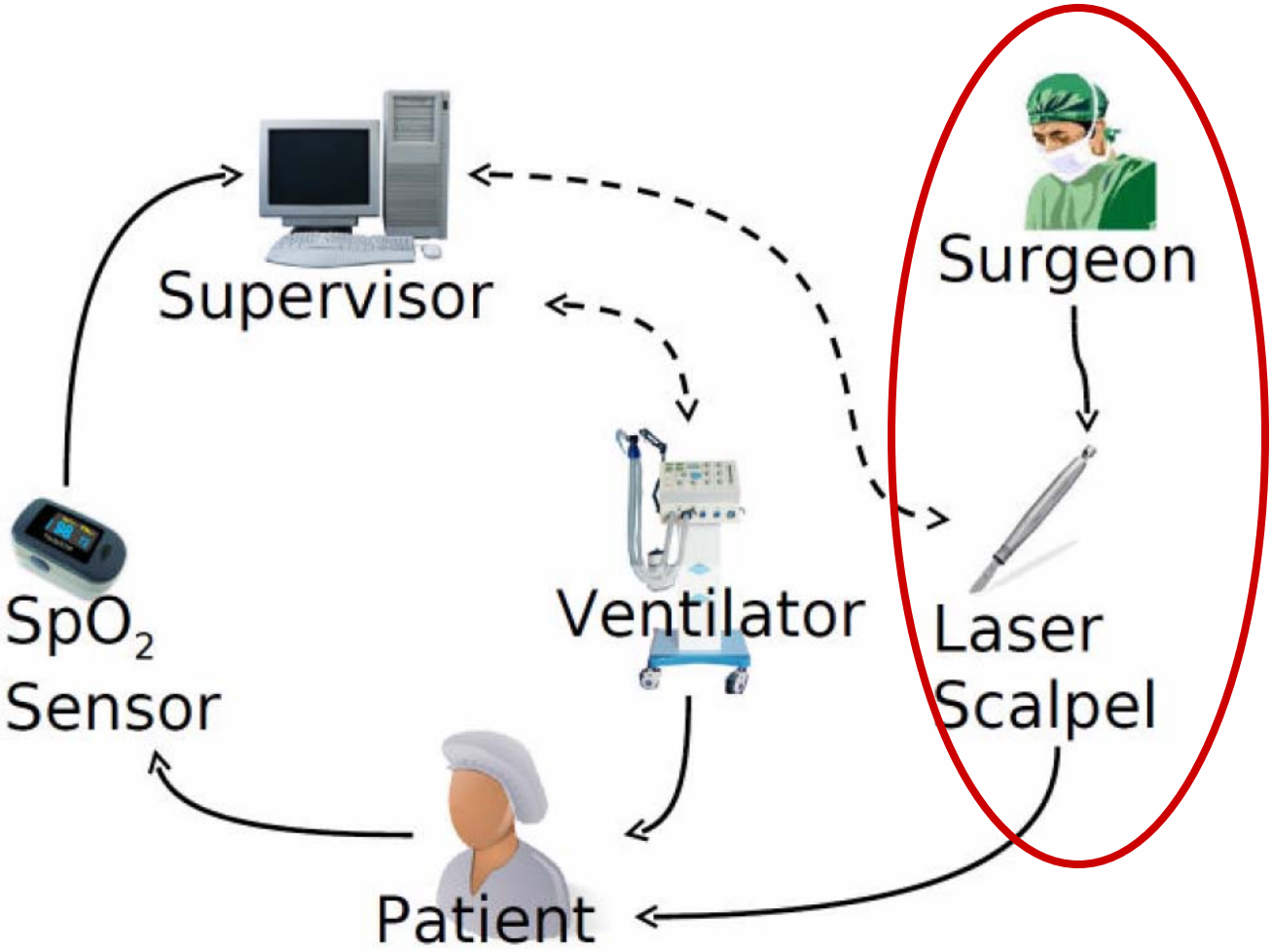
Laser Tracheotomy CPS PTE safety rule.



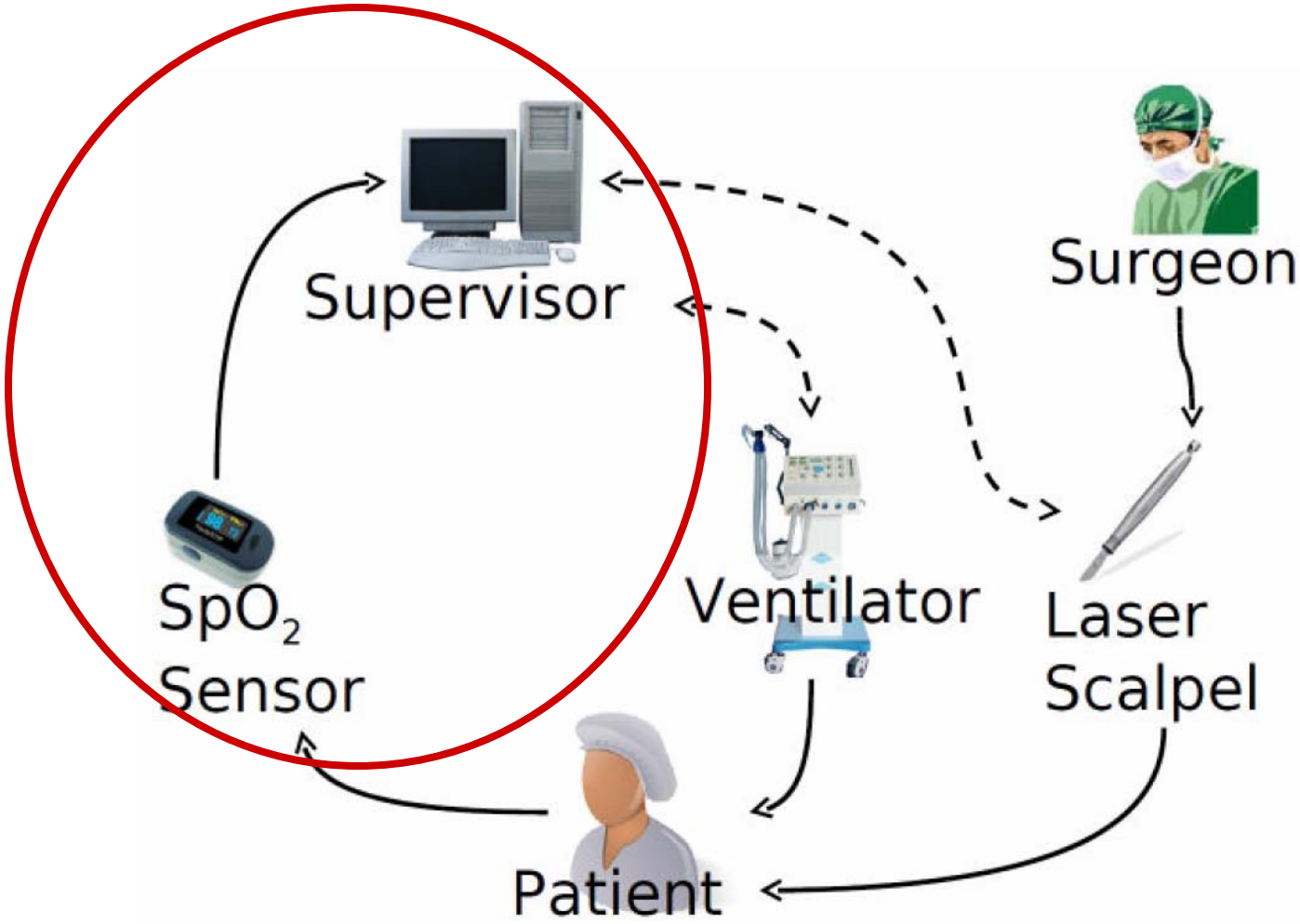
System architecture and roles of the design pattern: Initiator, Supervisor, Participant



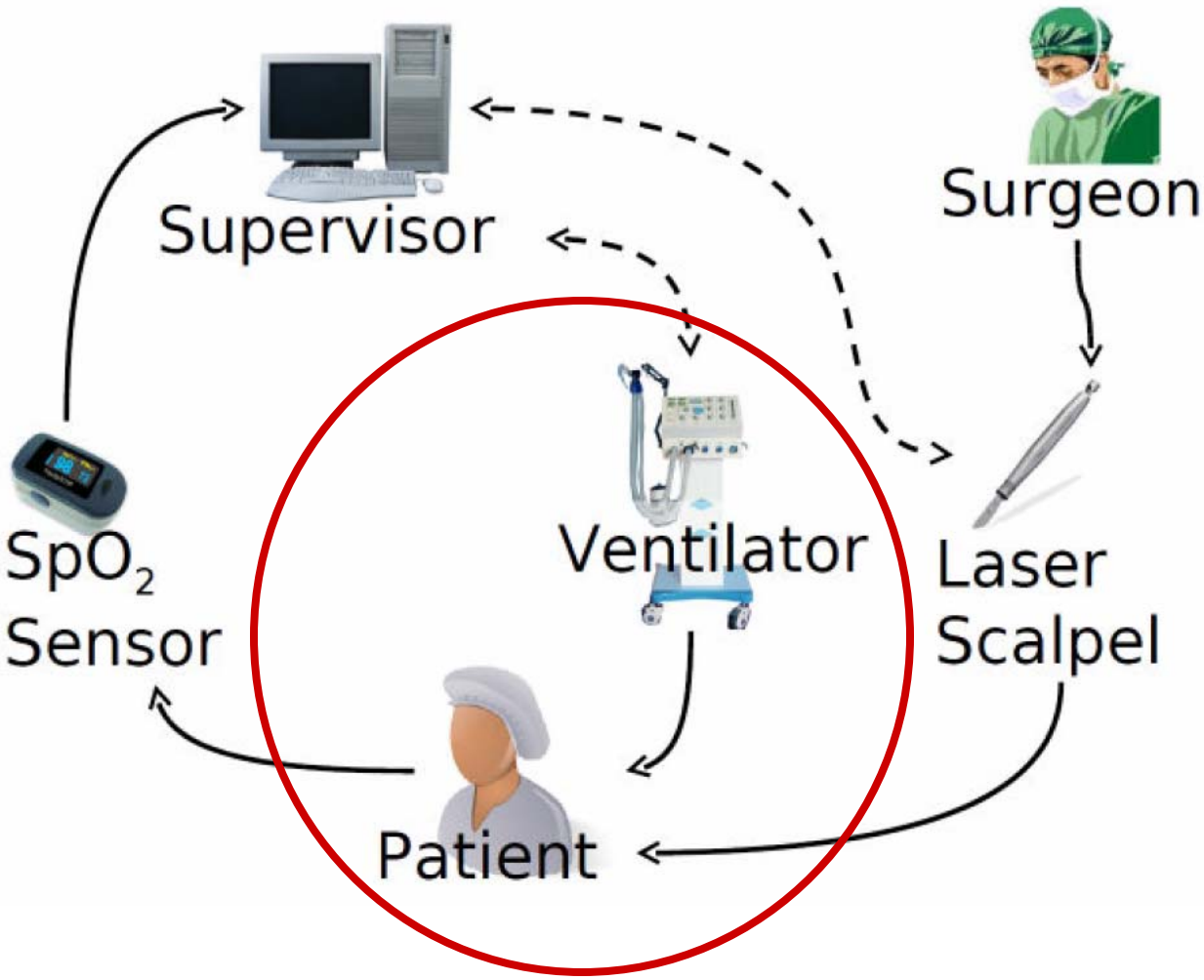
System architecture and roles of the design pattern: Initiator, Supervisor, Participant



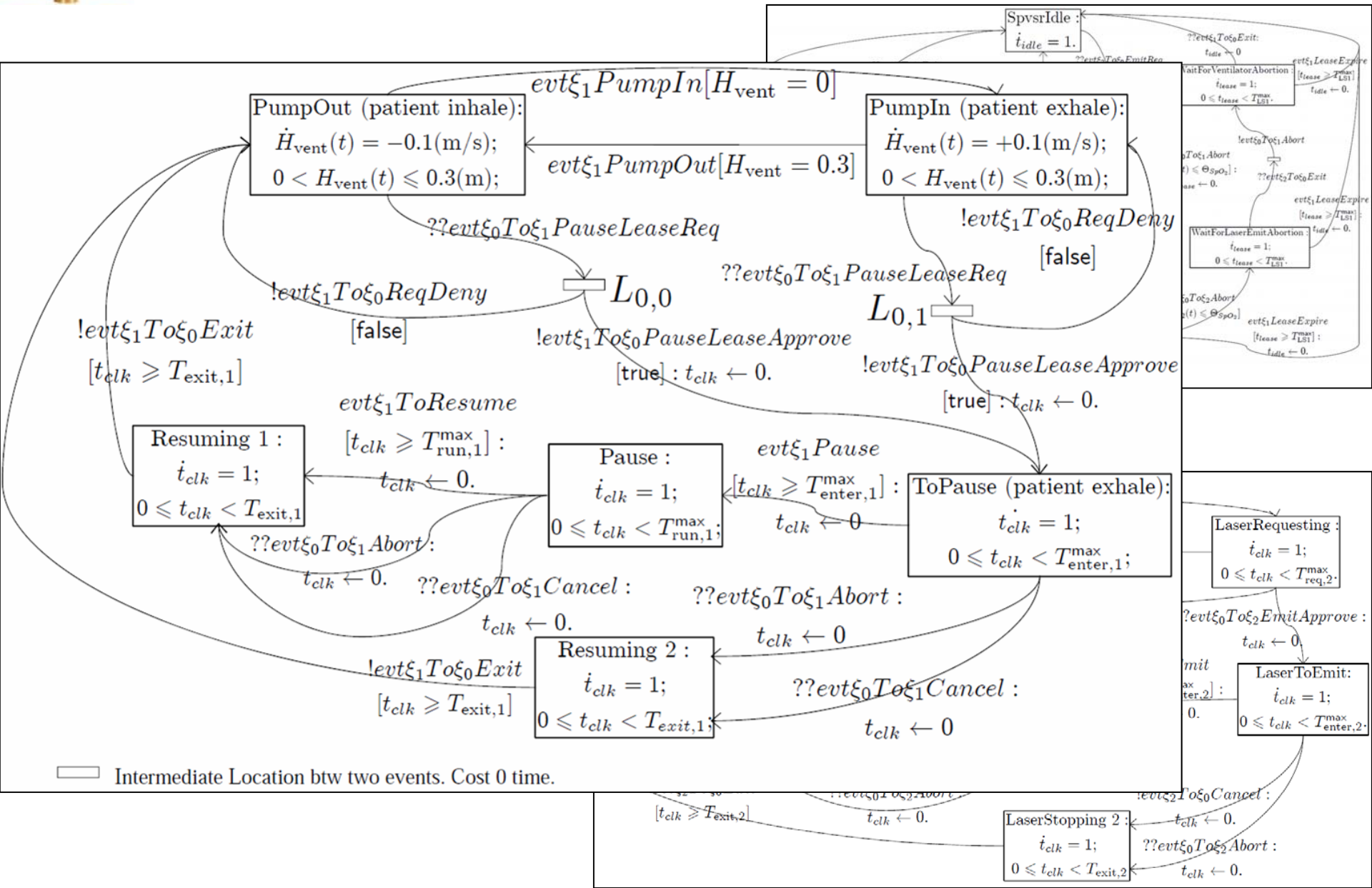
System architecture and roles of the design pattern: Initiator, Supervisor, Participant



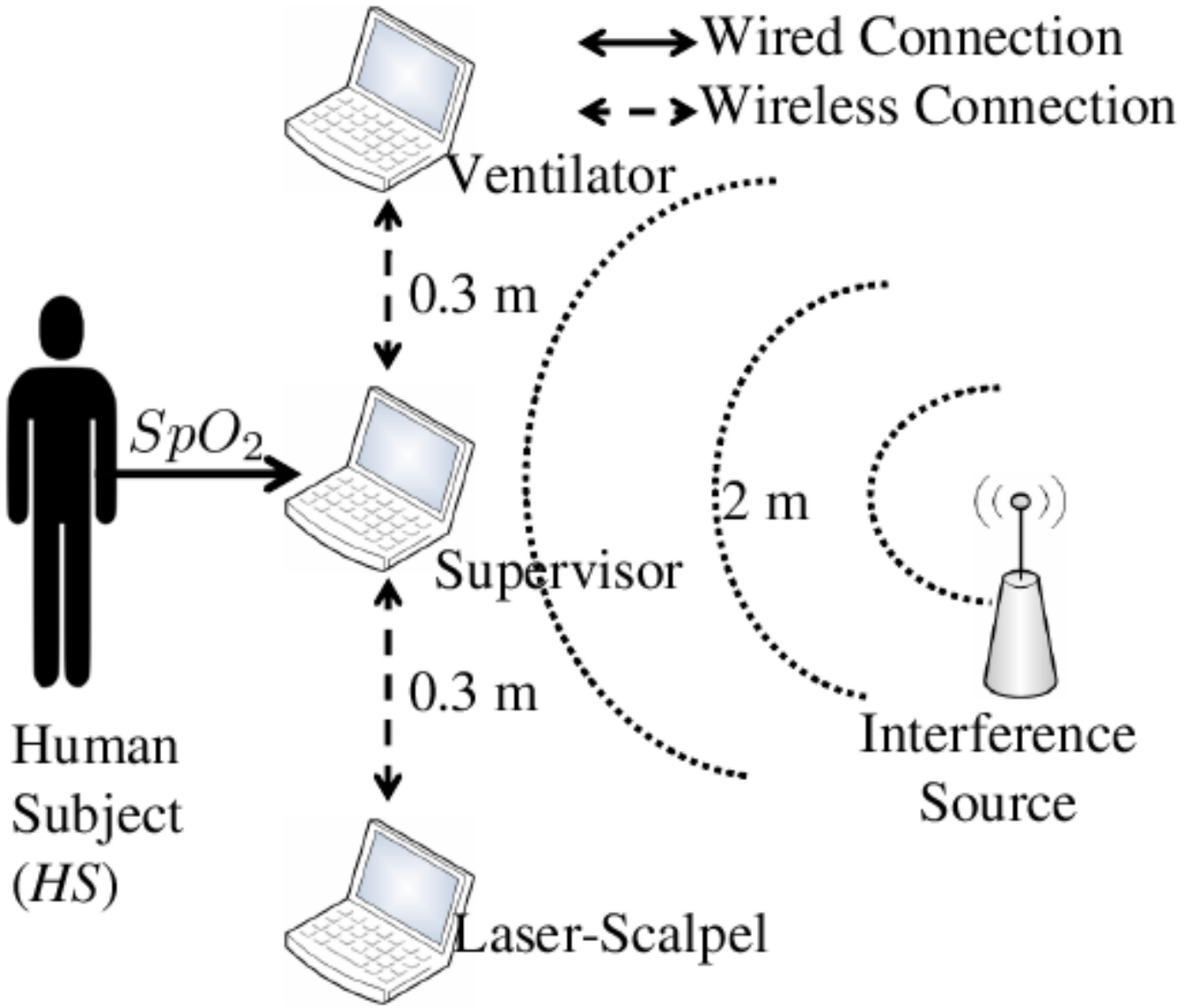
System architecture and roles of the design pattern: Initiator, Supervisor, Participant



Following the Leasing design pattern and Elaboration procedure, we derive detailed designs



Emulation Scheme



Emulation Results

Trial Mode	$E(T_{\text{off}})$ (sec)	# of Laser Emissions	# of Failures	# of $evtToStop$
with Lease	18	19	0	5
without Lease	18	11	4	0
with Lease	6	19	0	3
without Lease	6	12	3	0

1. Each trial lasts 30 minutes, and is under constant WiFi interference.
2. For each trial, the expectation $E(T_{\text{on}}) \equiv 30$(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

Surgical Medicine

Anesthesiology

Nursing

Computer

Communications

Mechanics

Control

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

Chemical Engineering

Control

Mechanics

Computer

Thermal Engineering

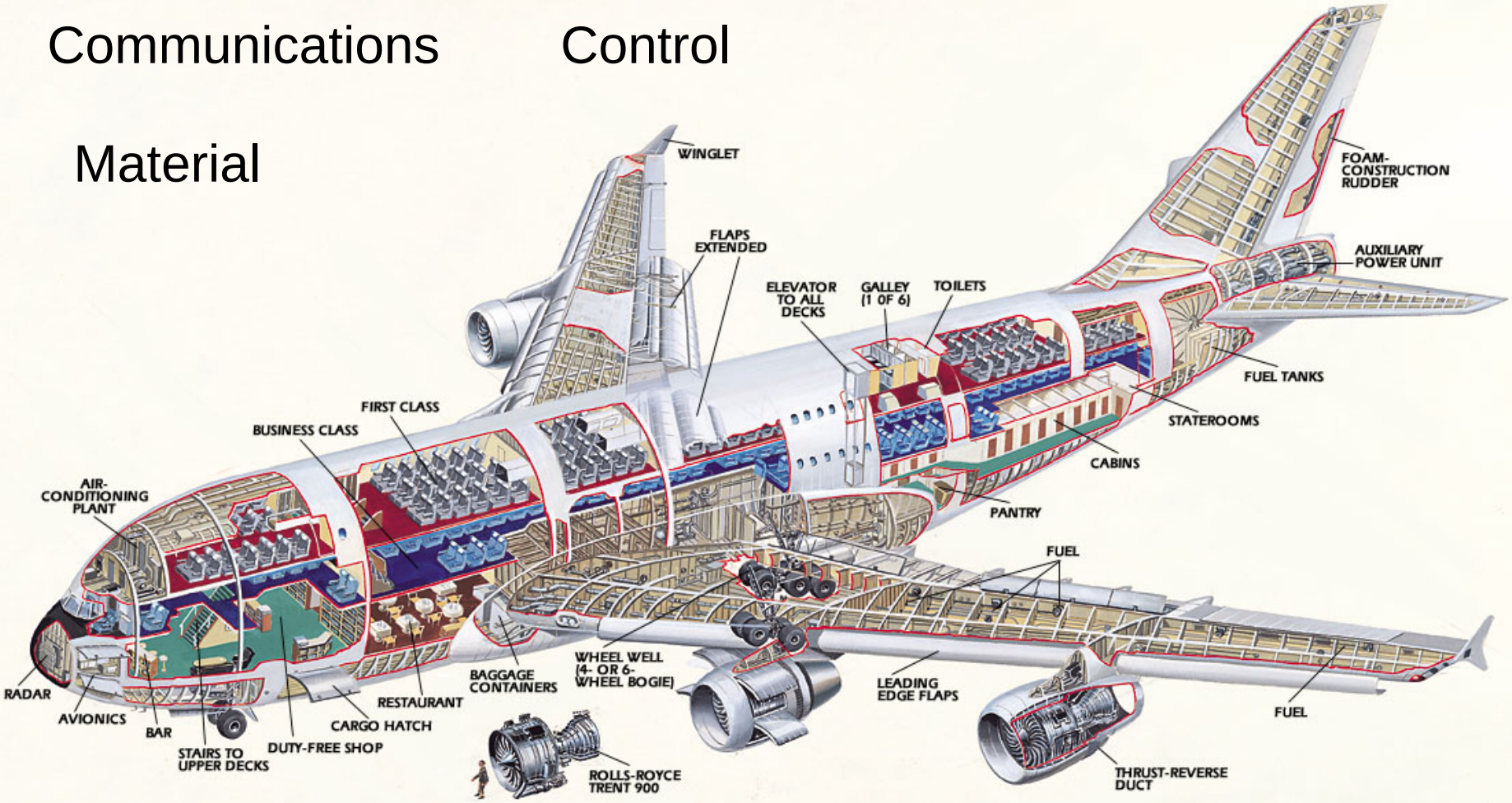
Communications

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

Computer Mechanics Aerodynamics

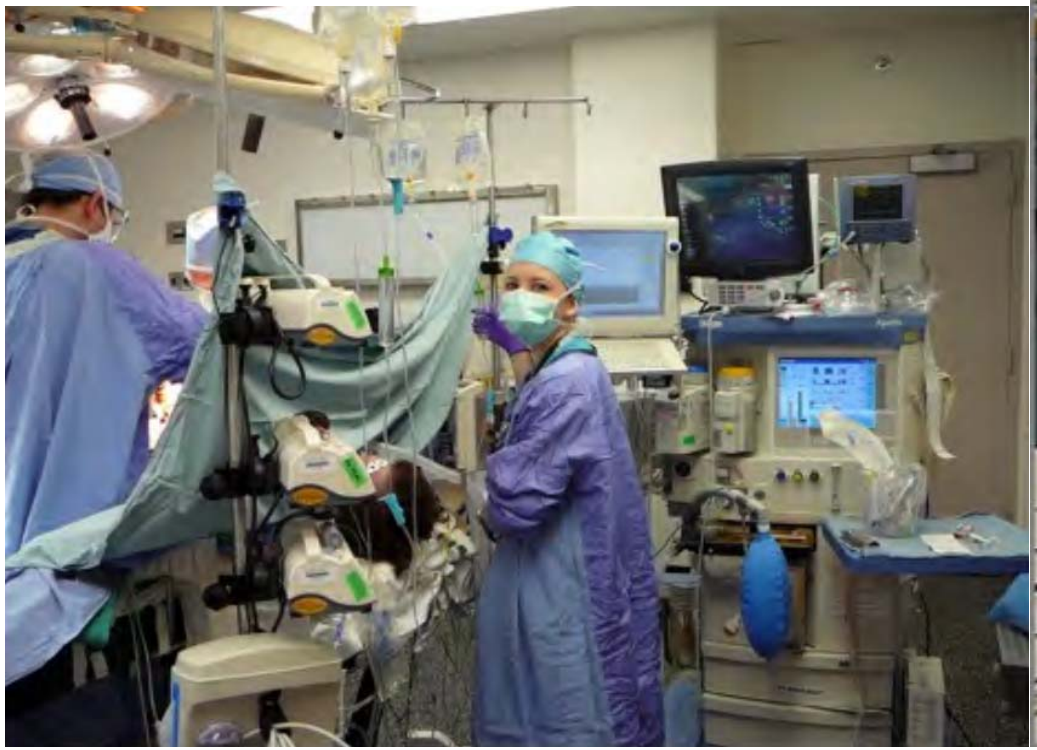
Communications Control

Material



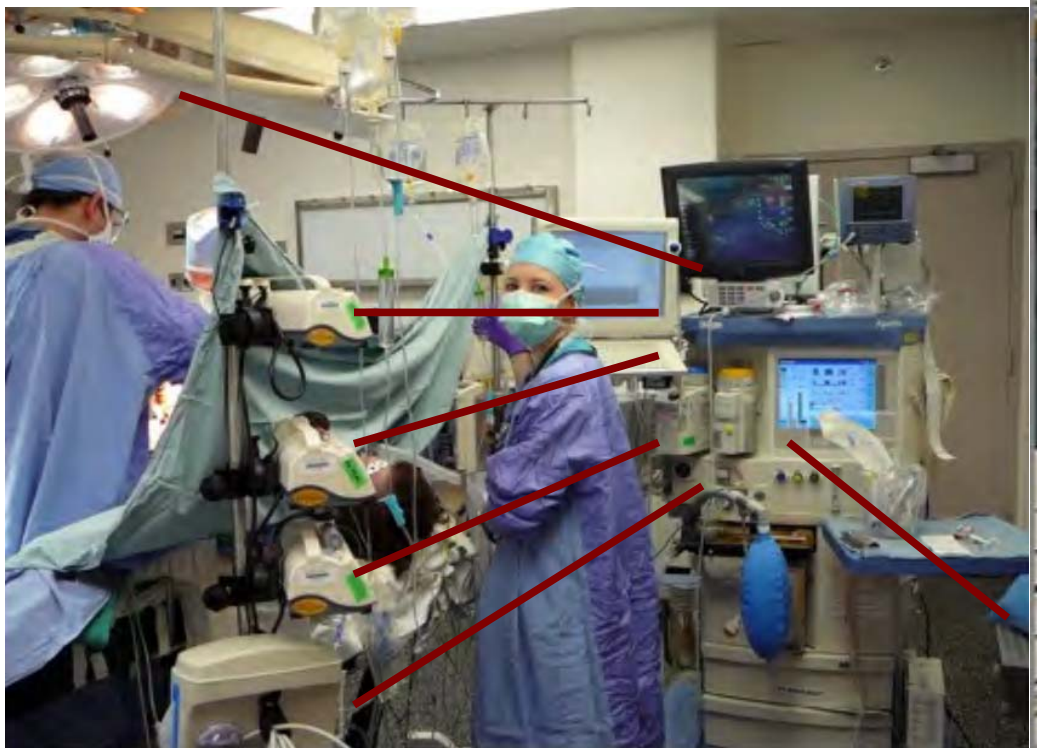
Demand to use wireless links for safety and efficiency concerns.

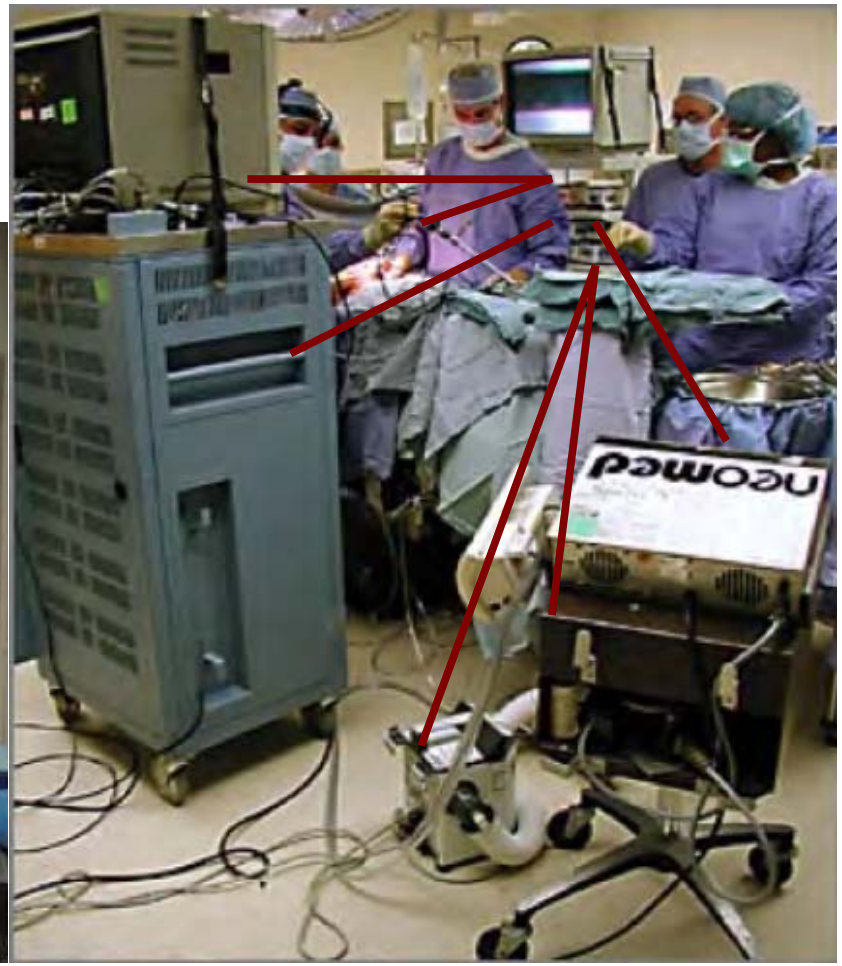
The Operation Room Spider Web



Demand to use wireless links for safety and efficiency concerns.

The Operation Room Spider Web, after medical CPS safety interlocks

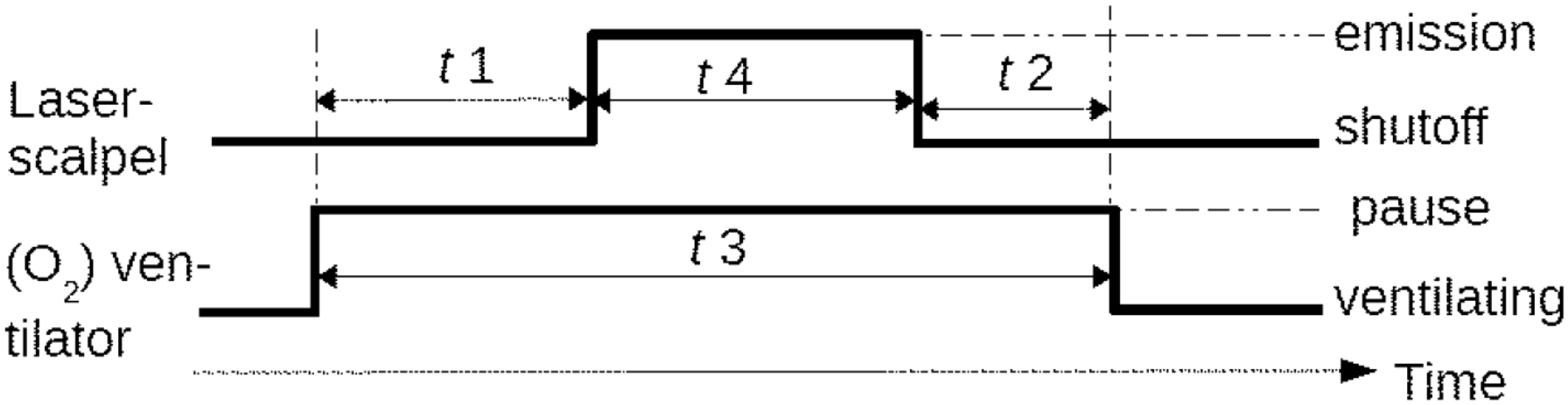




Demand to use wireless links for safety and efficiency concerns.

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

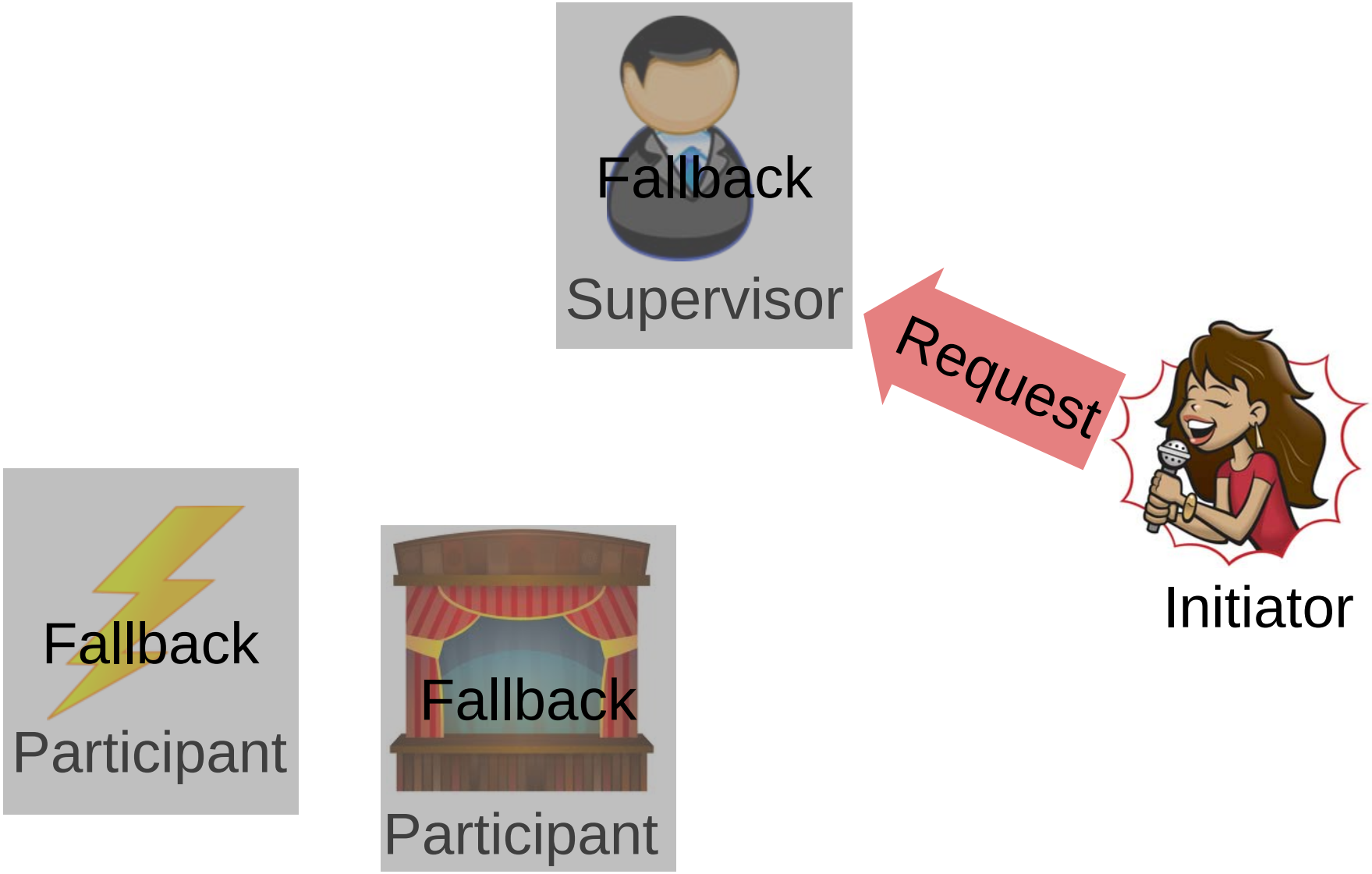
Initiator

Participant

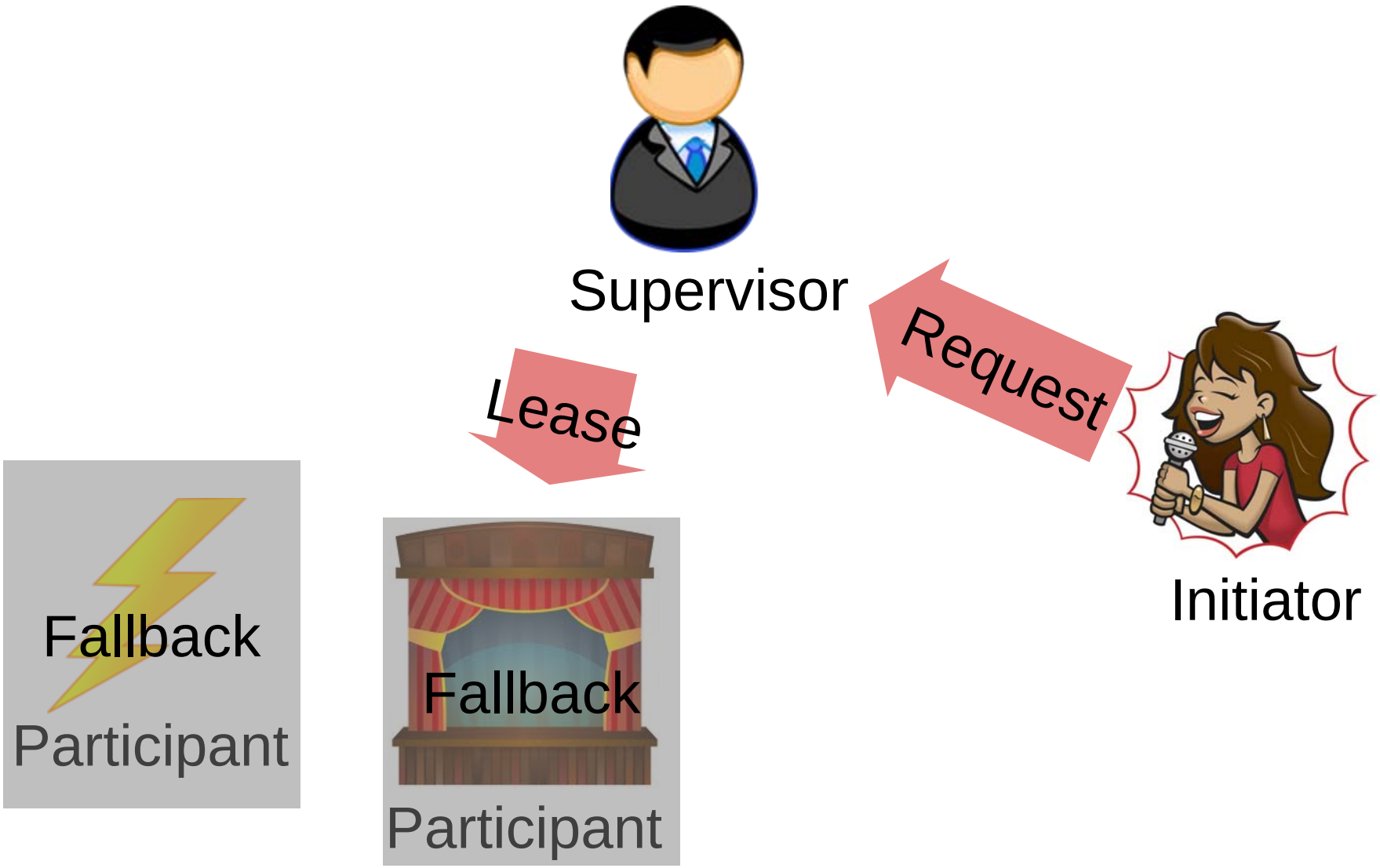
Participant

General concept of Leasing Design Pattern for CPS PTE guarantee

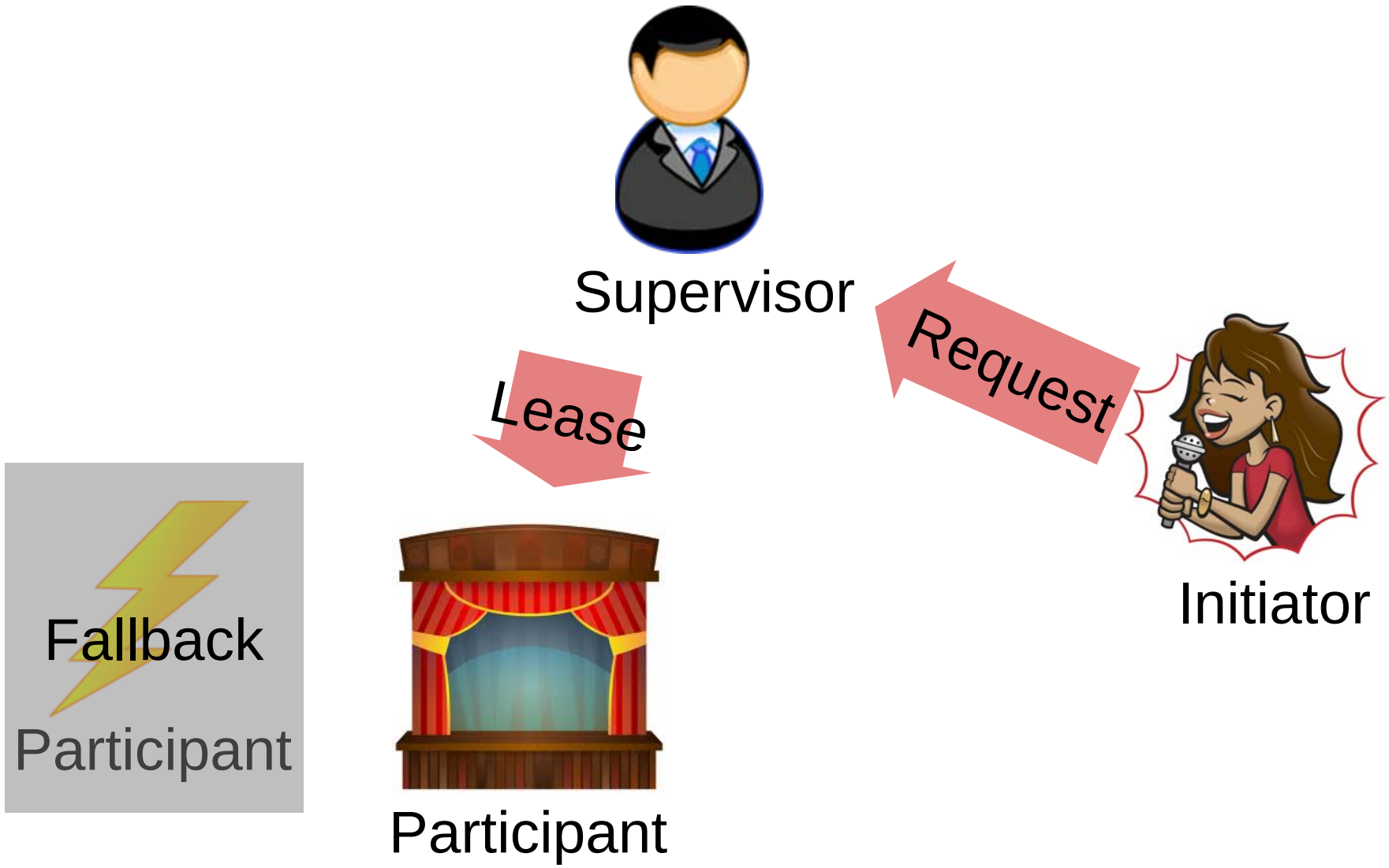
General concept of Leasing Design Pattern for CPS PTE guarantee



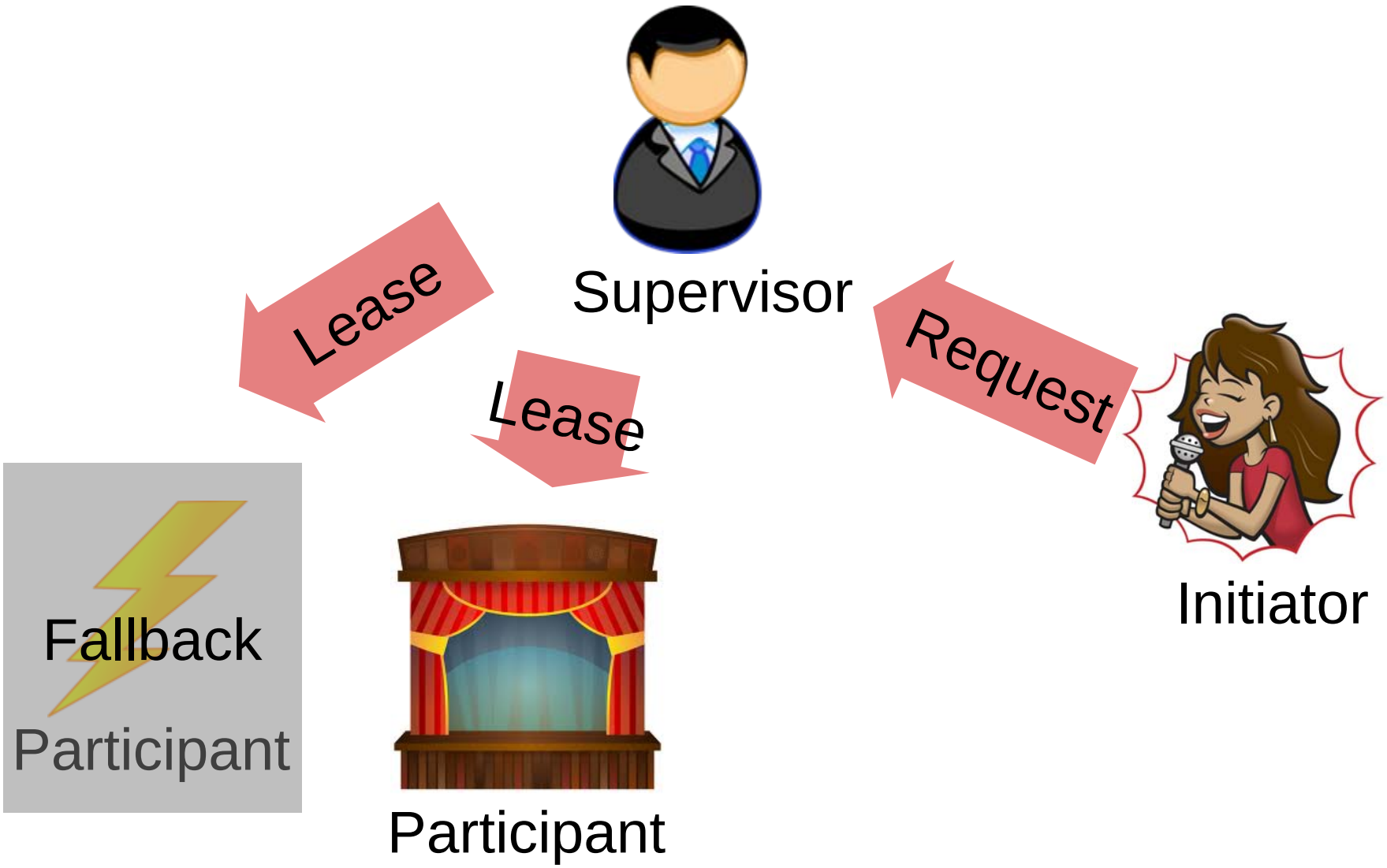
General concept of Leasing Design Pattern for CPS PTE guarantee



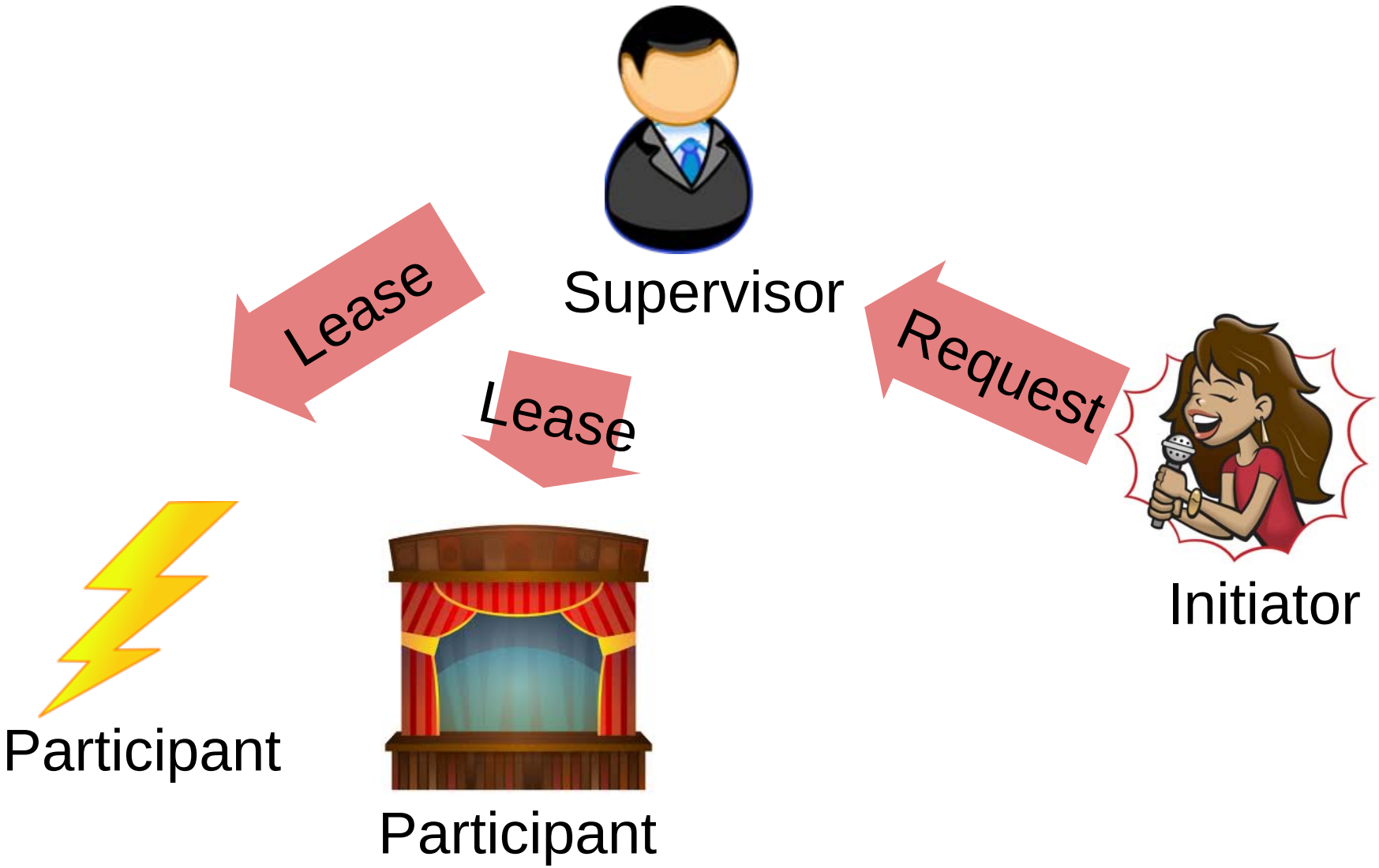
General concept of Leasing Design Pattern for CPS PTE guarantee



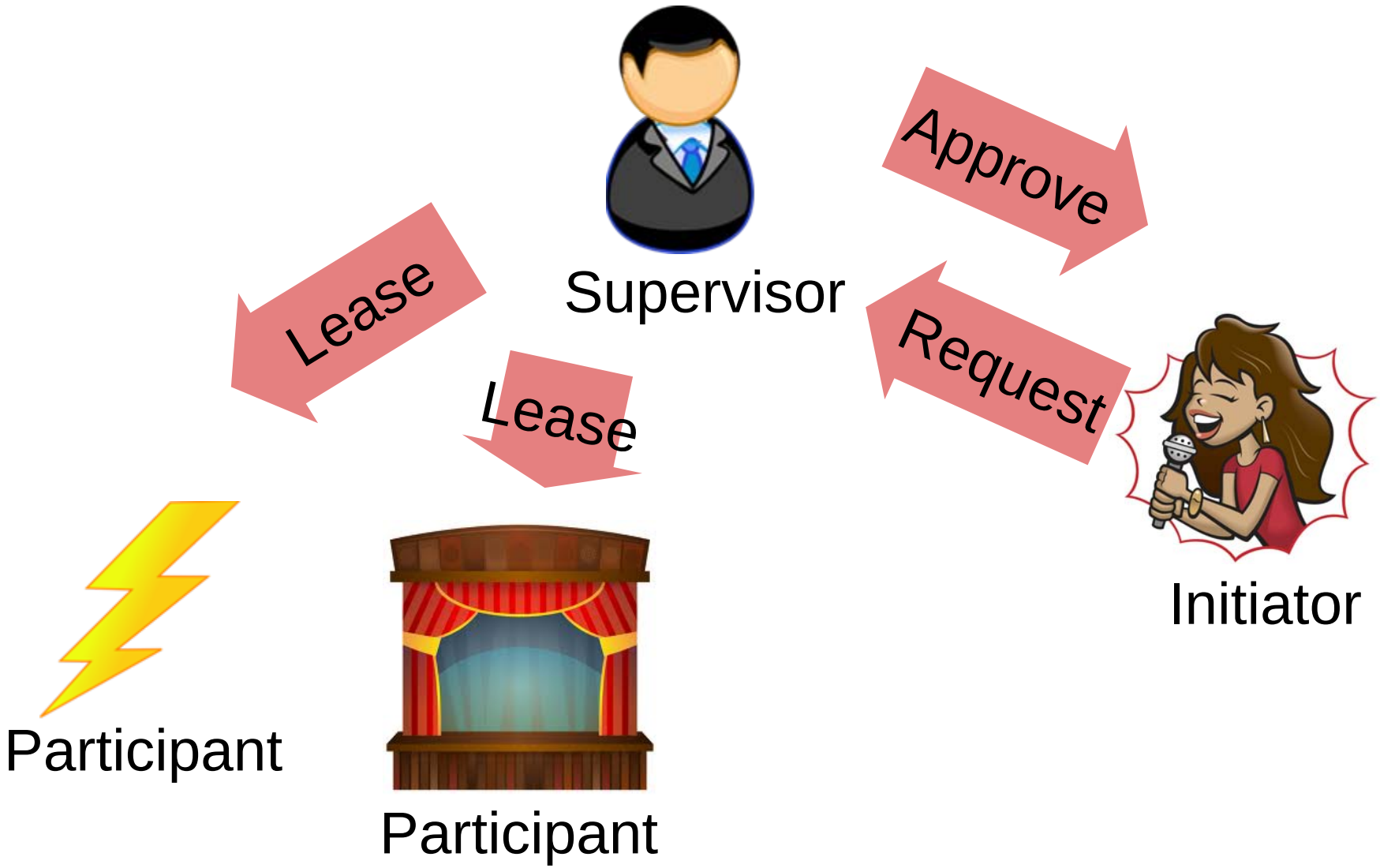
General concept of Leasing Design Pattern for CPS PTE guarantee



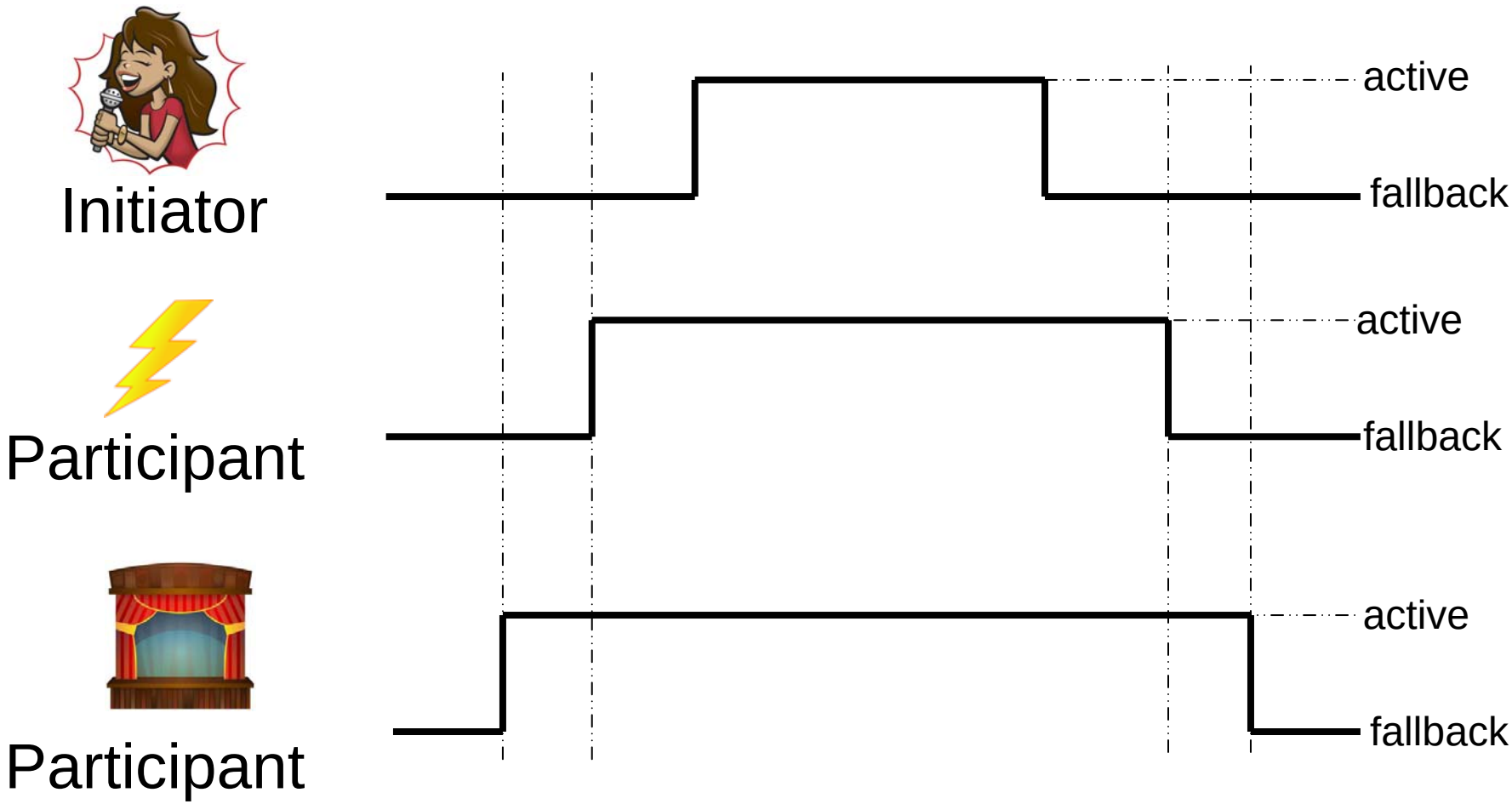
General concept of Leasing Design Pattern for CPS PTE guarantee



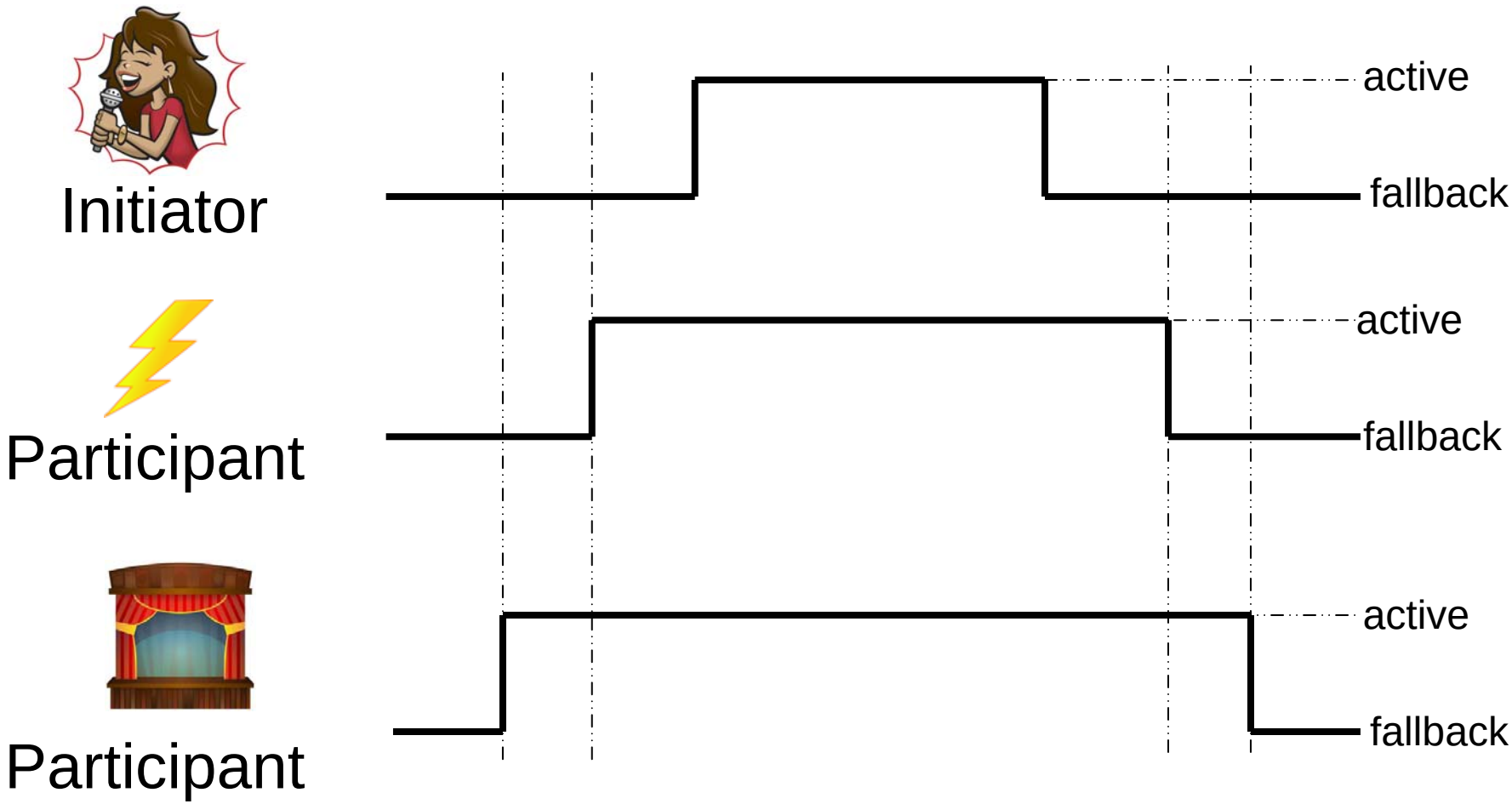
General concept of Leasing Design Pattern for CPS PTE guarantee



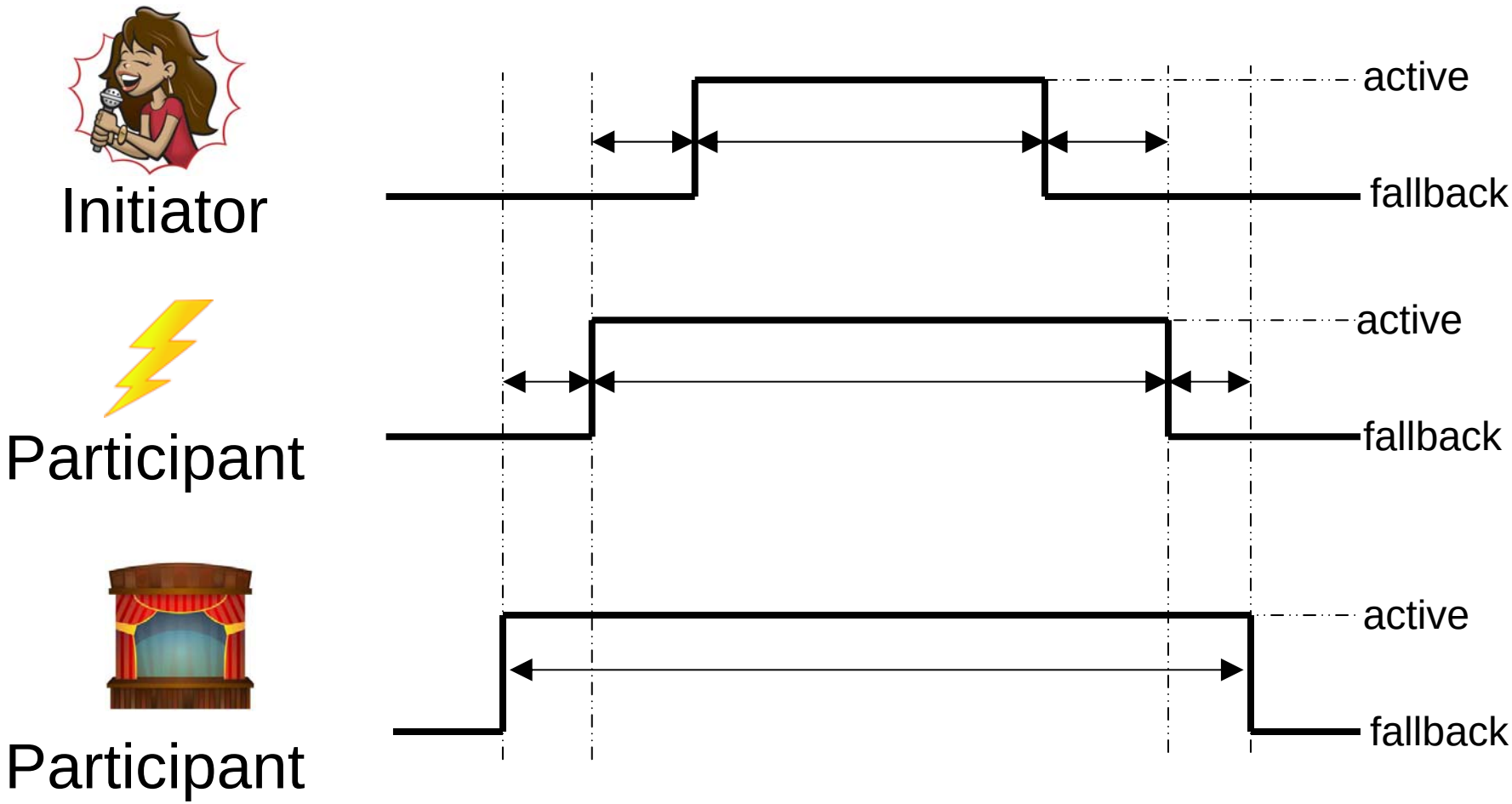
General concept of Leasing Design Pattern for CPS PTE guarantee



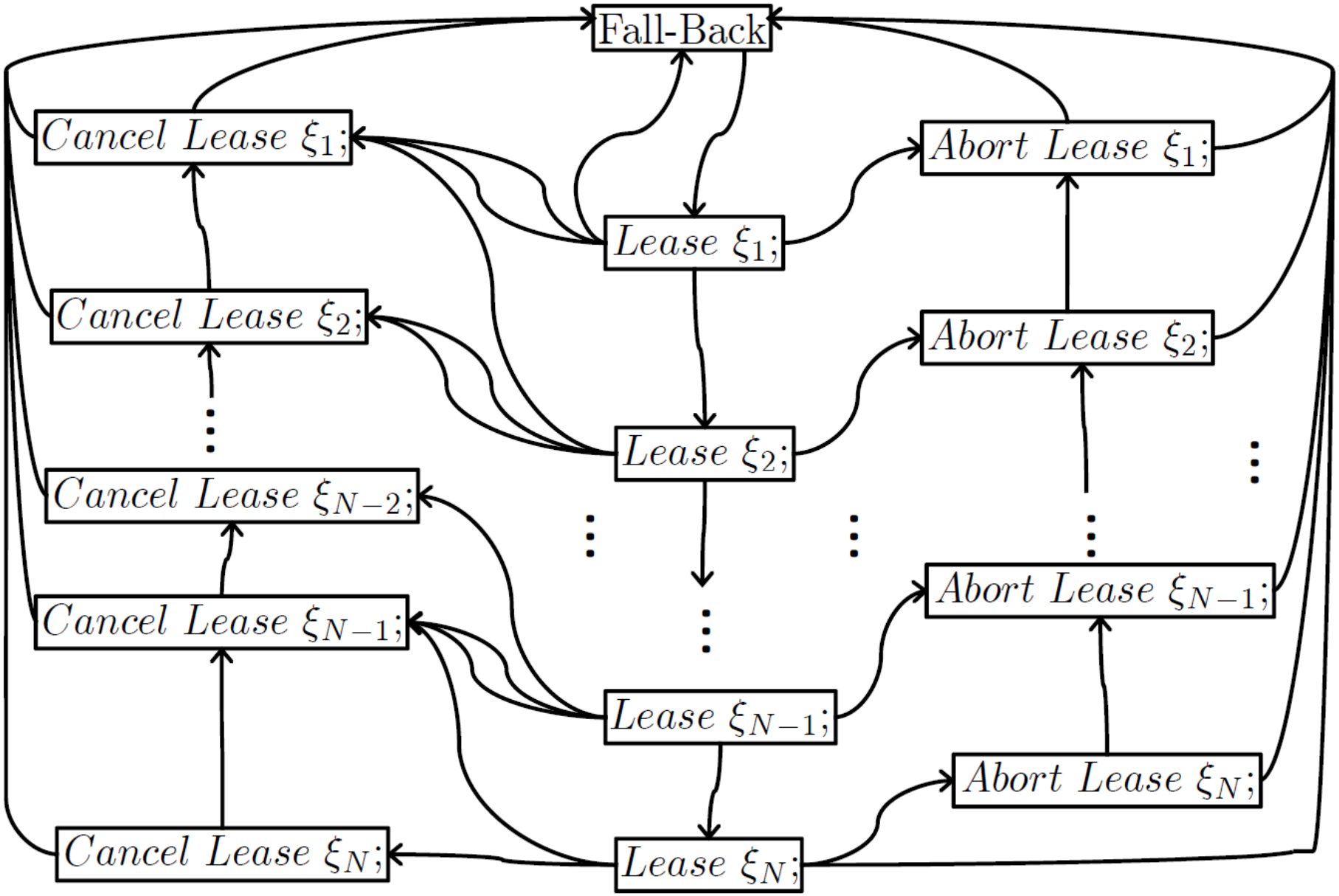
The same scenario can also apply to purely cyber systems. What's the difference that CPS makes?



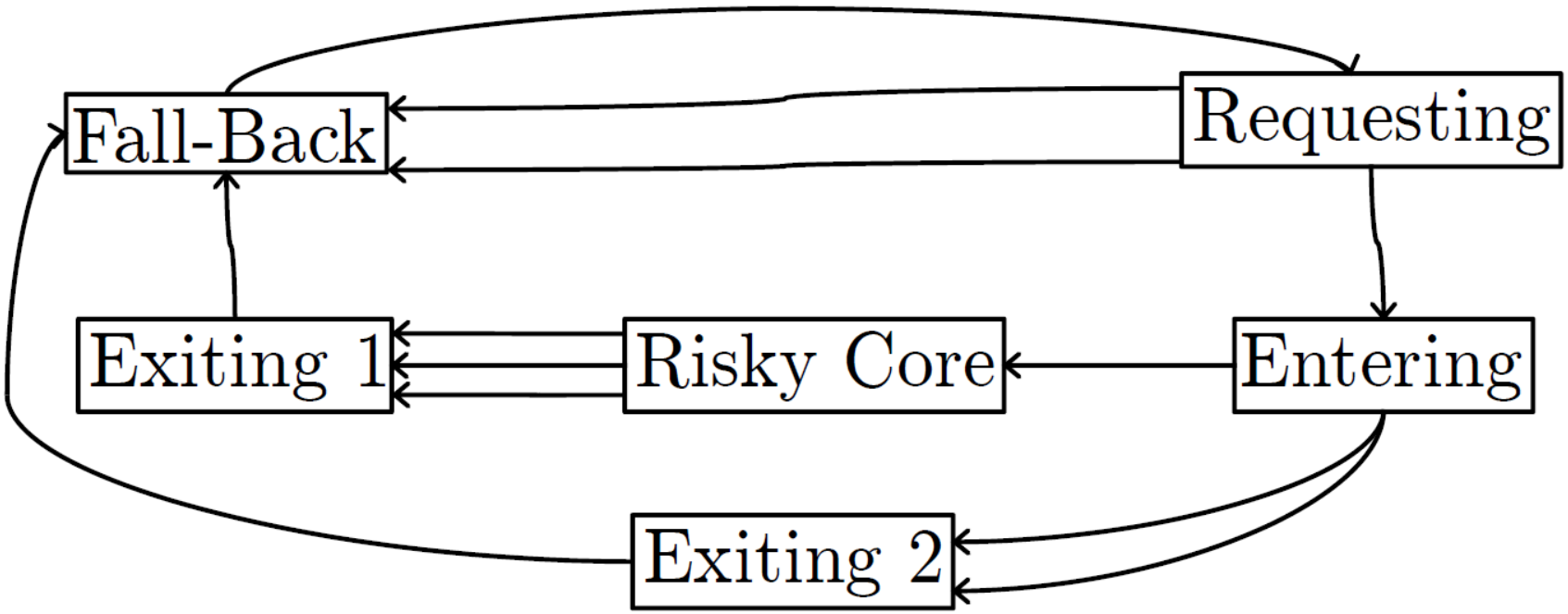
CPS Features: 1. real-time matters; 2. real-time PTE even when aborting/canceling. (+ 3. arbitrary comm. failures)



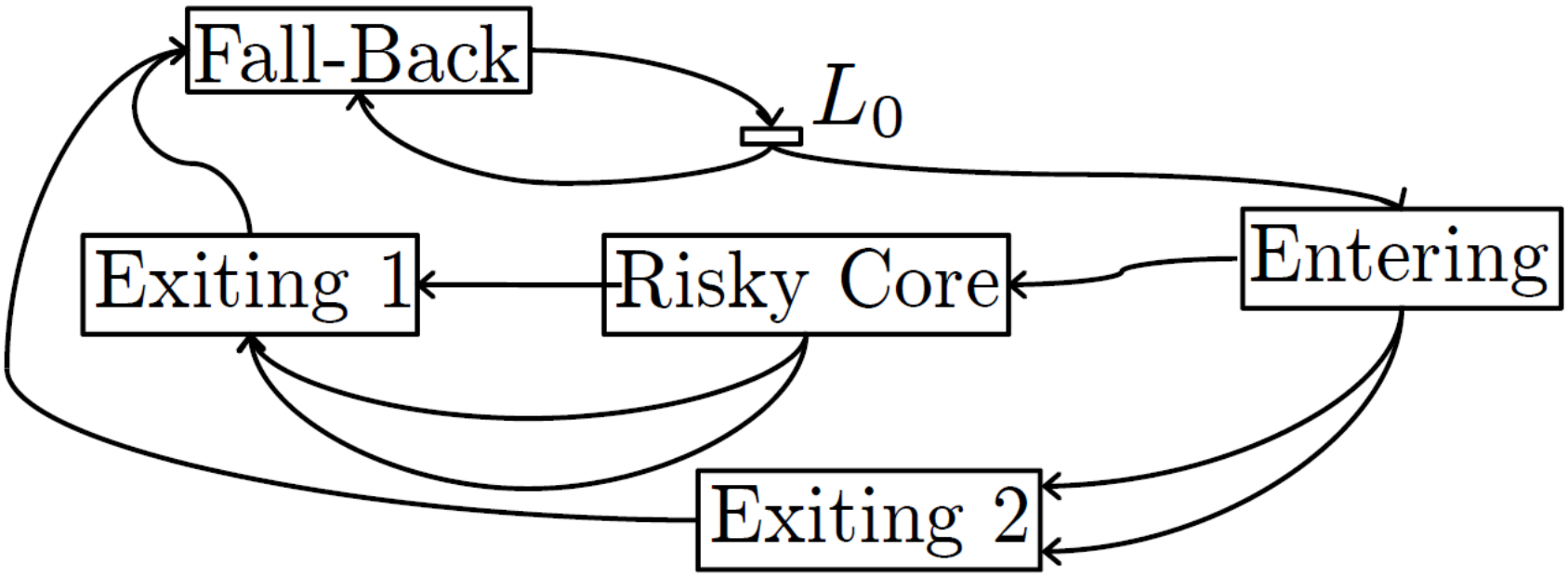
Leasing Design Pattern for PTE Safety Rules: sketch of Supervisor's hybrid automaton



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

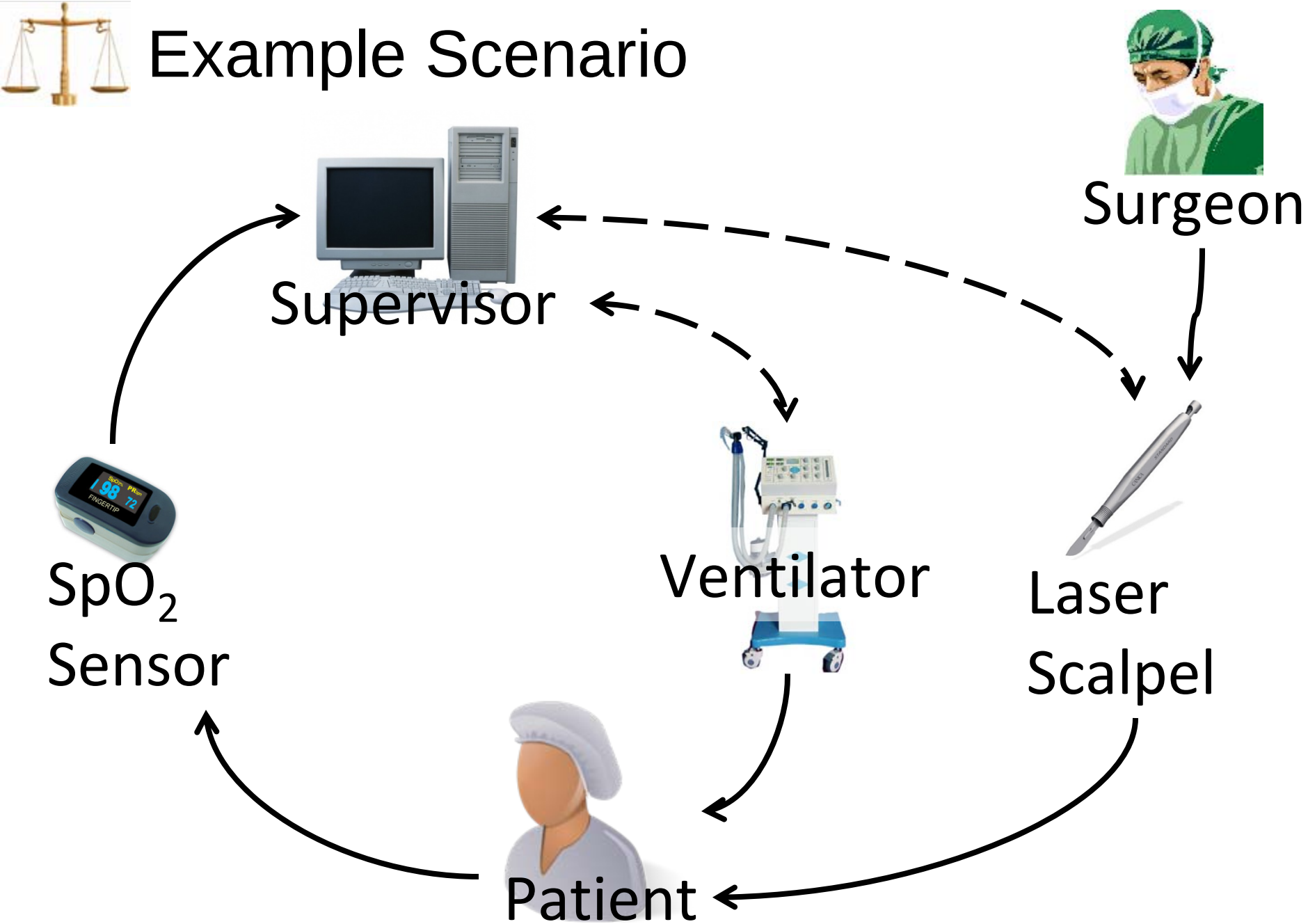
$$\text{Supervisor}: T_{fb,0}^{\min} = 13(s), T_{wait}^{\max} = 3(s)$$

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

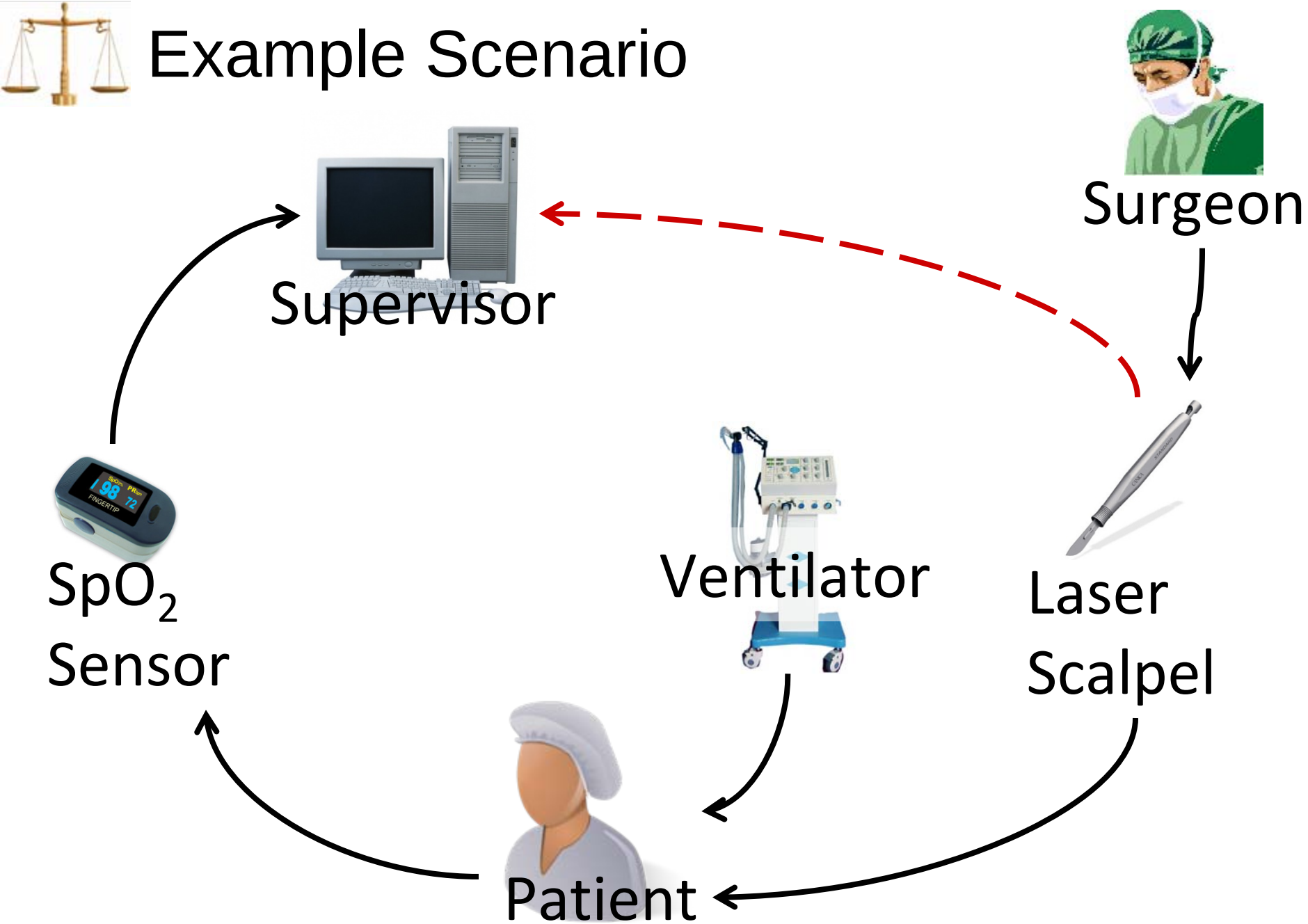
$$\text{Ventilator}: T_{enter,1}^{\max} = 3(s), T_{run,1}^{\max} = 35(s), T_{exit,1} = 6(s)$$

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

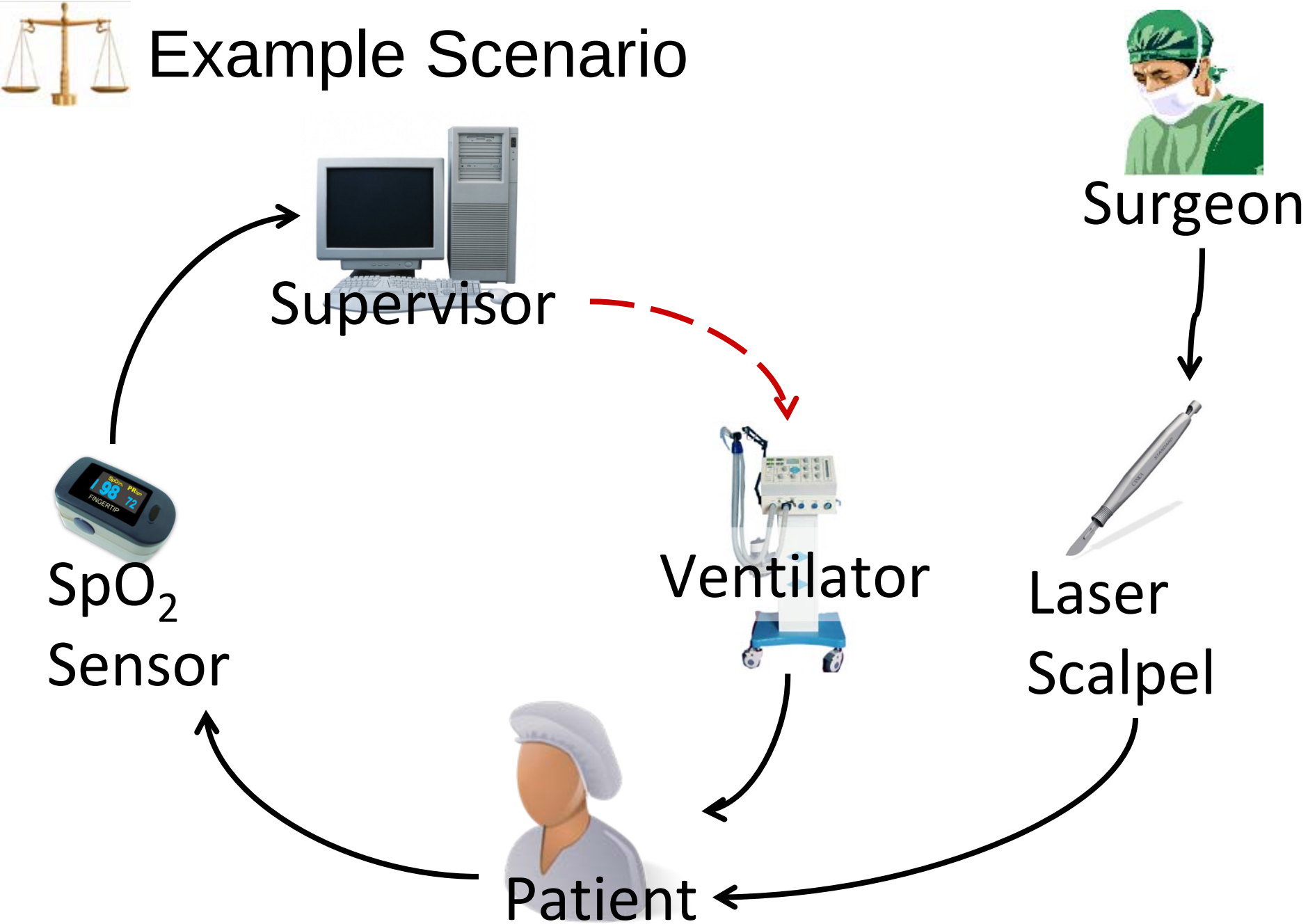
Example Scenario



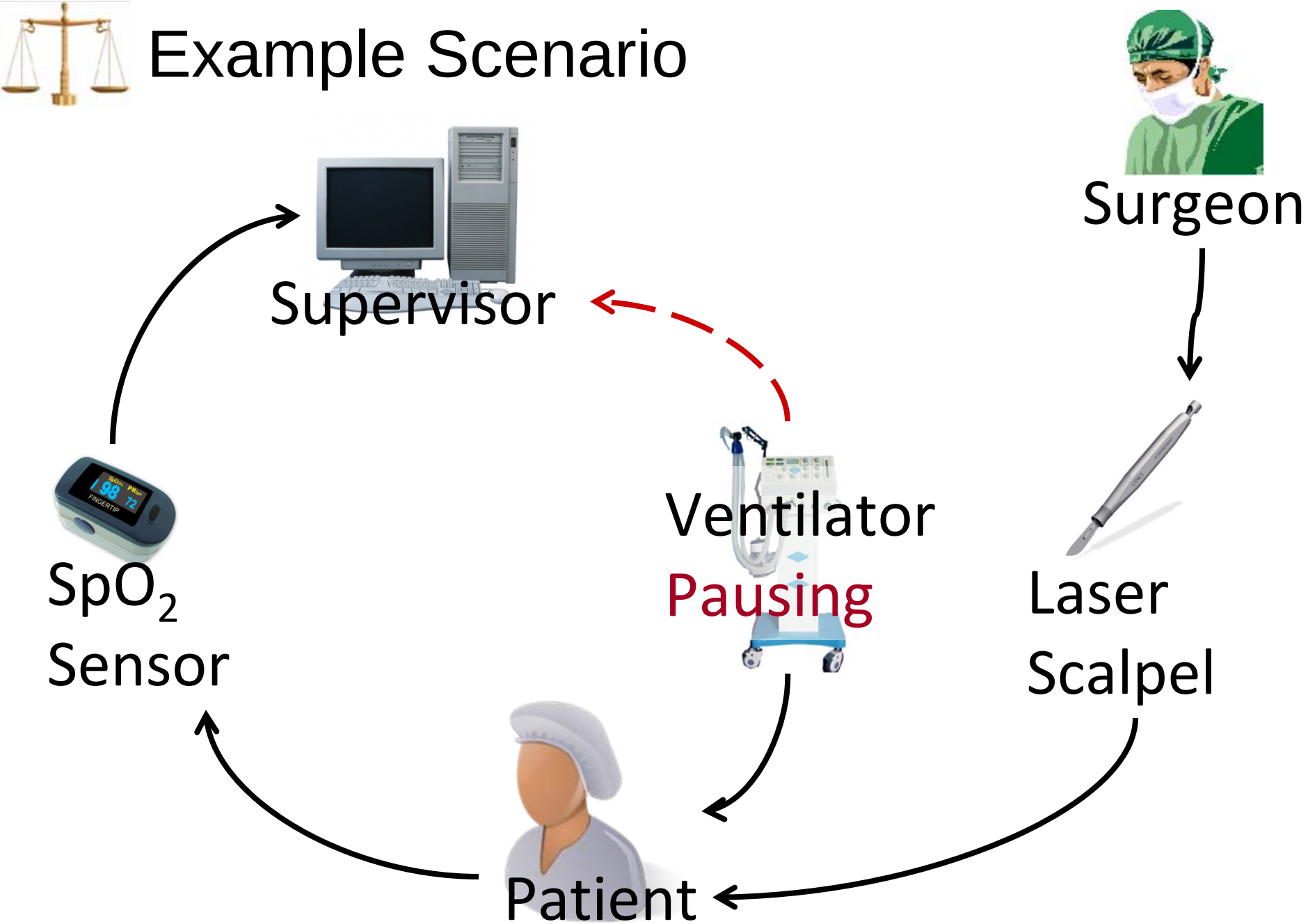
Example Scenario



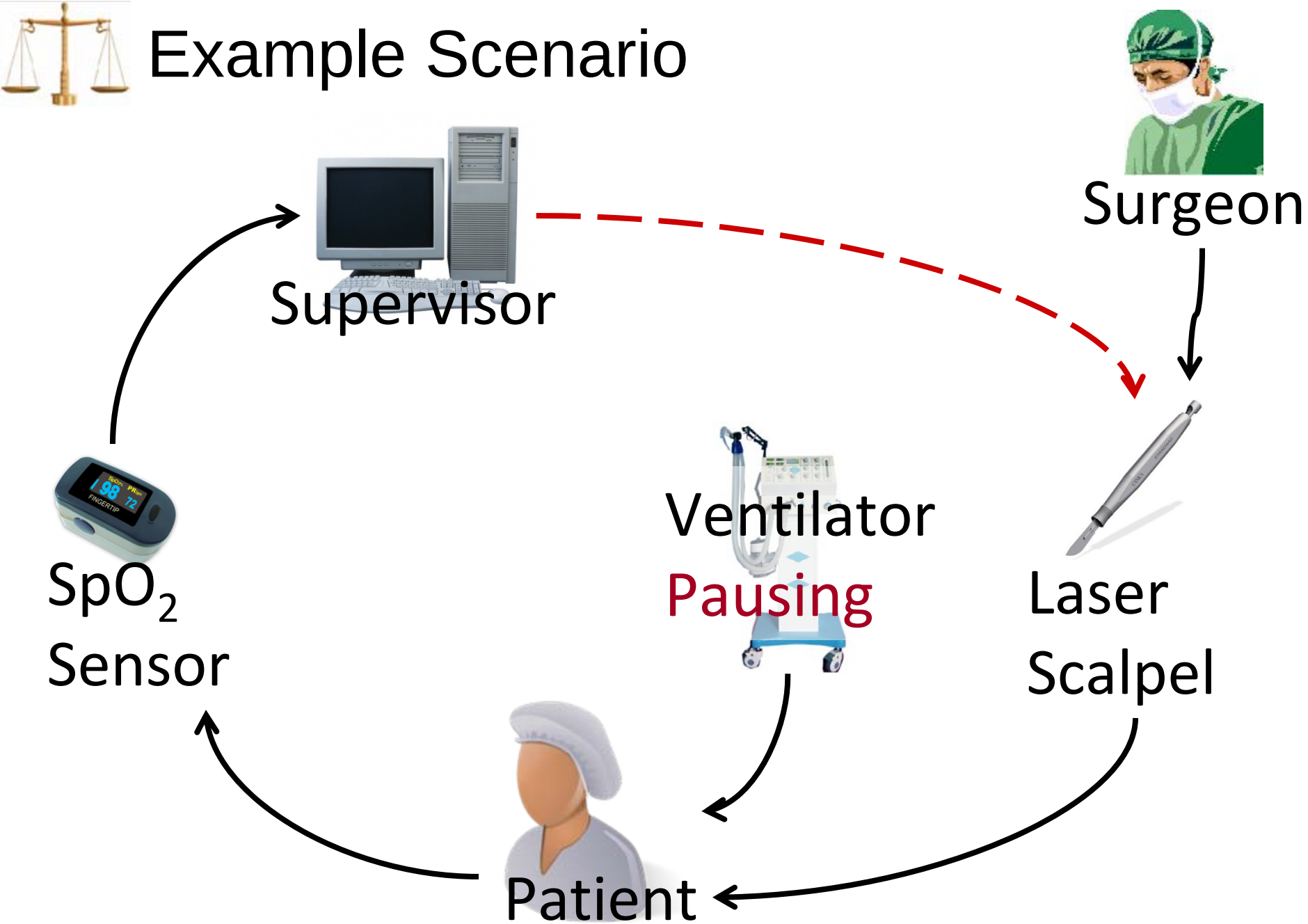
Example Scenario



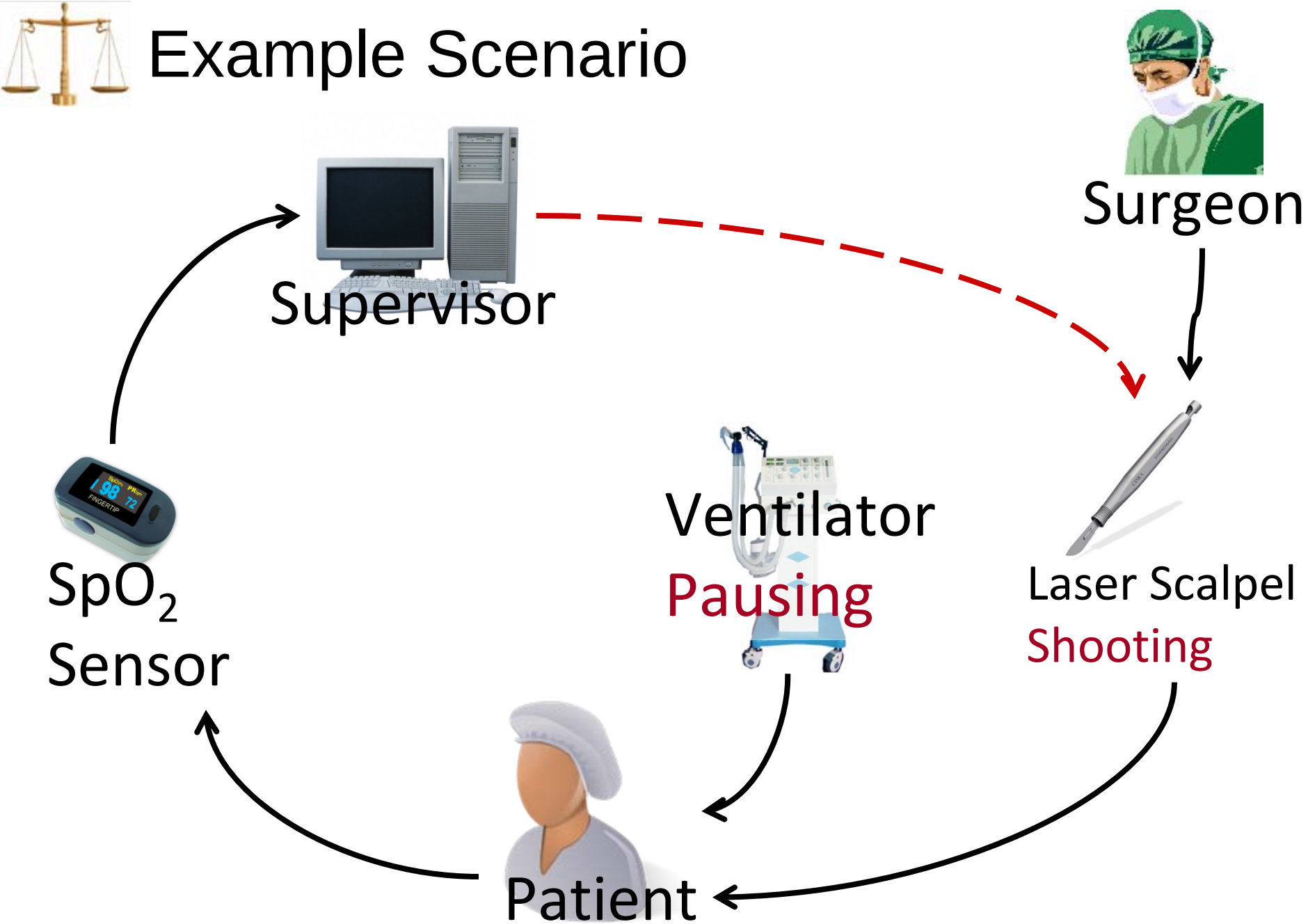
Example Scenario



Example Scenario



Example Scenario



Example Scenario

Surgeon

Supervisor

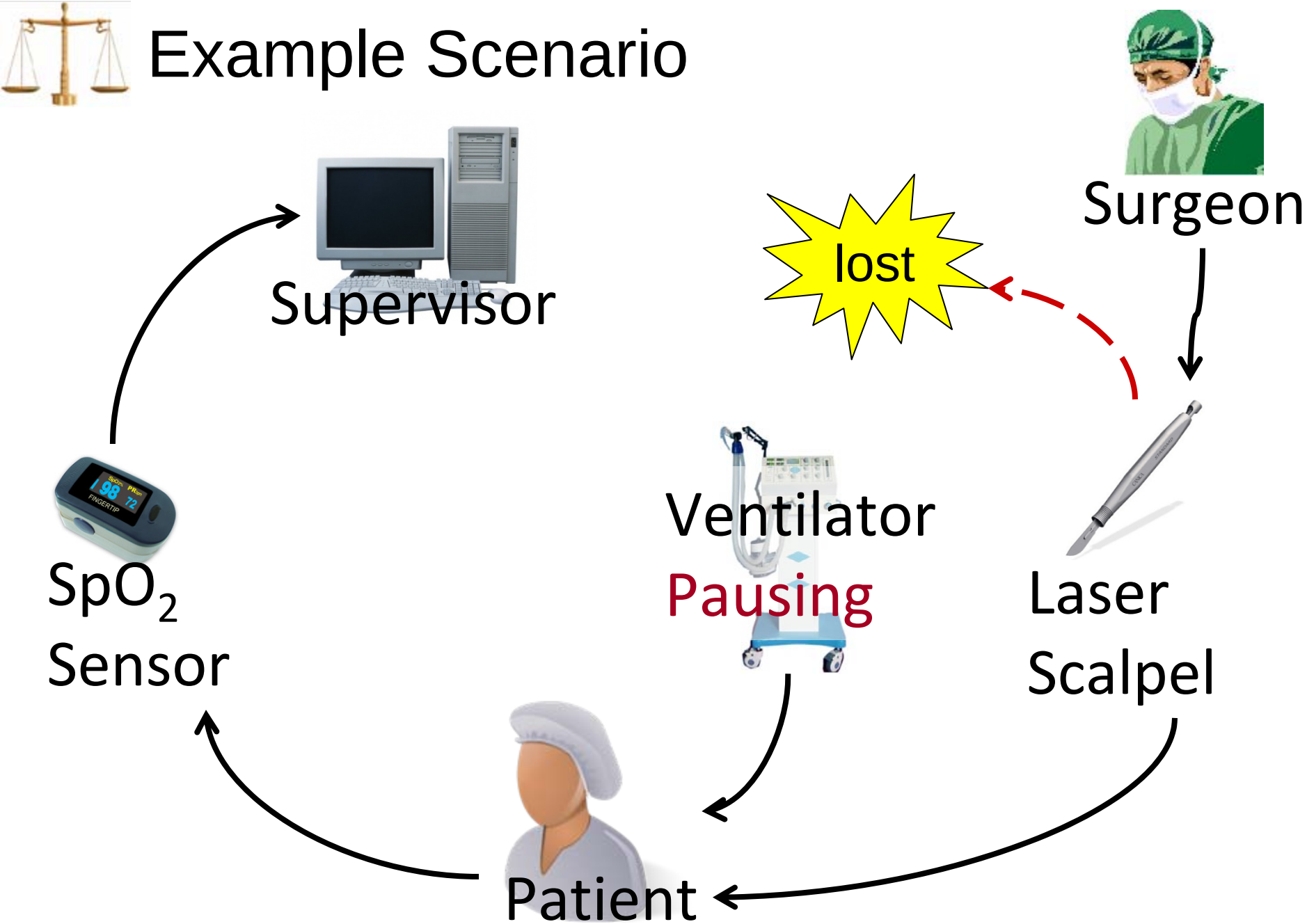
Laser Scalpel

Ventilator Pausing

SpO_2 Sensor

Patient

Example Scenario



Example Scenario

Surgeon

Supervisor

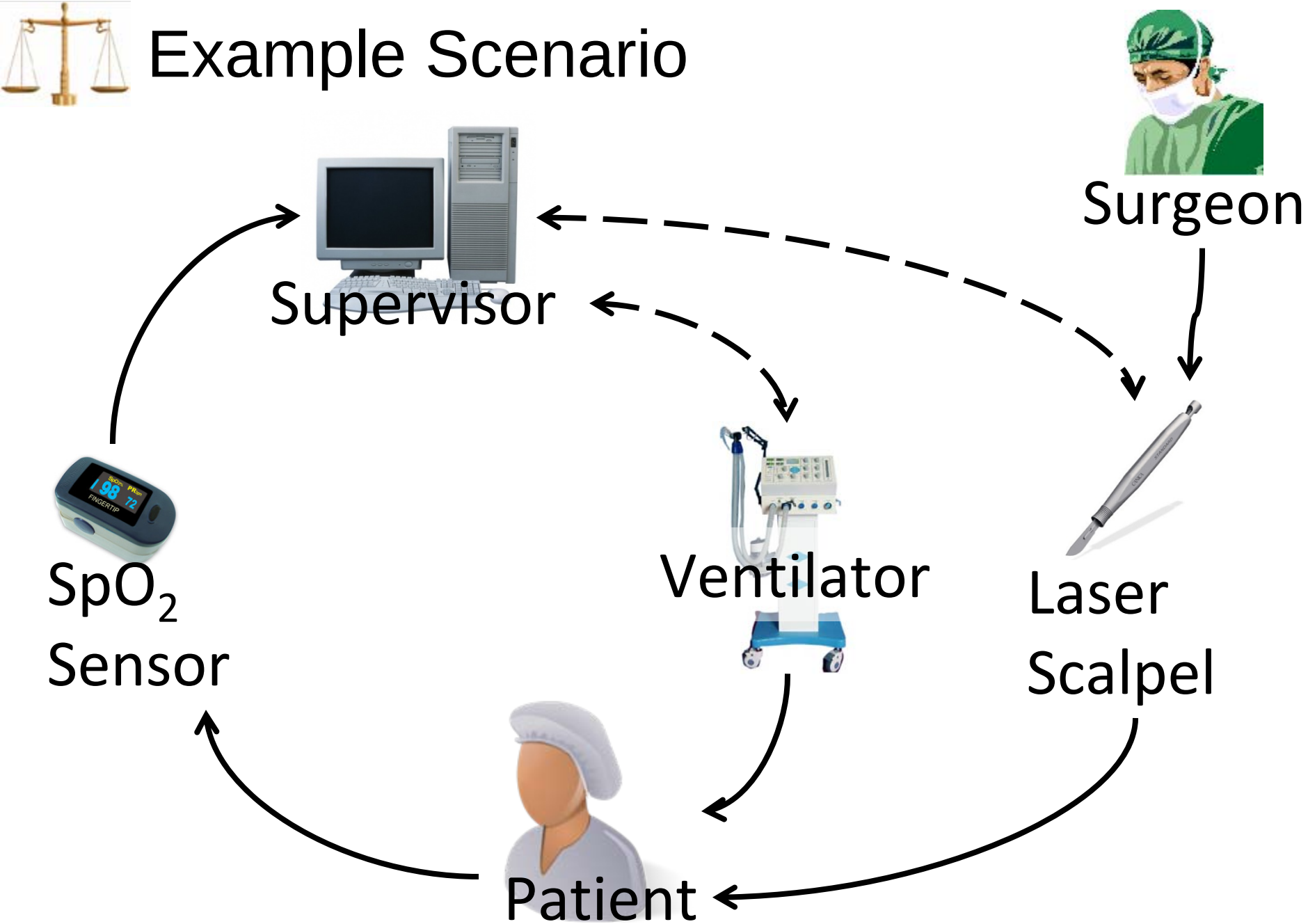
Laser Scalpel

Ventilator Pausing

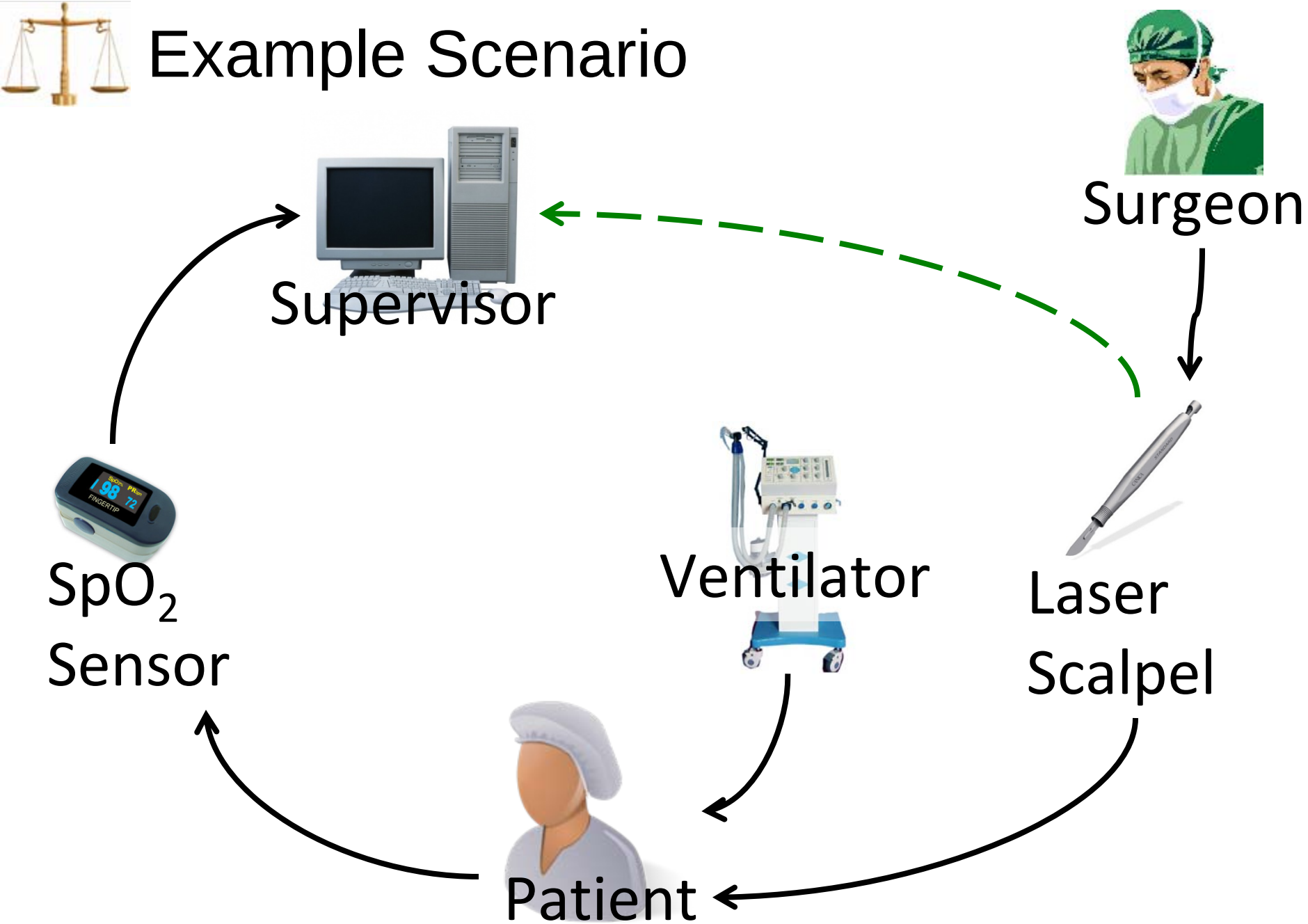
SpO_2 Sensor

Patient

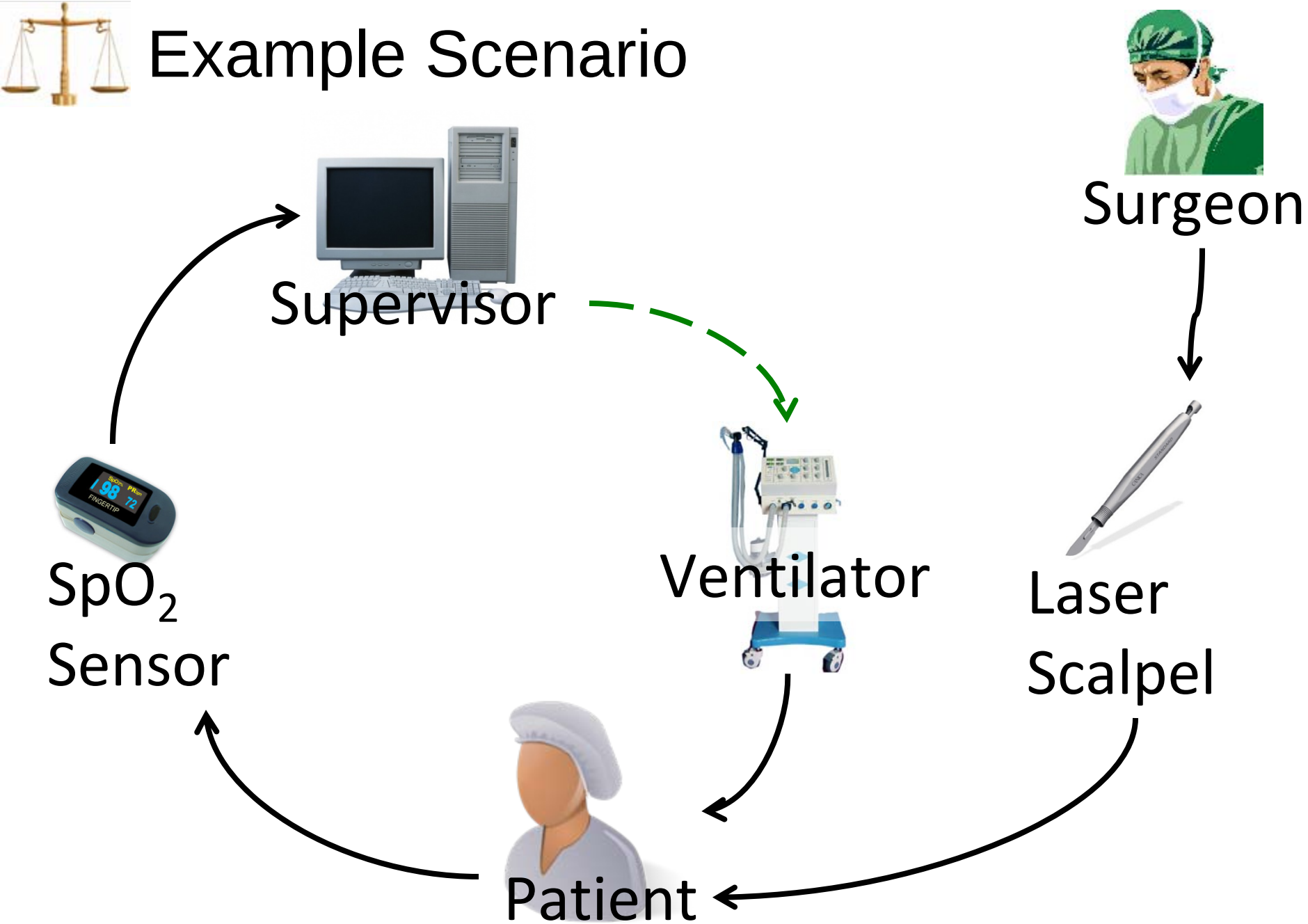
Example Scenario



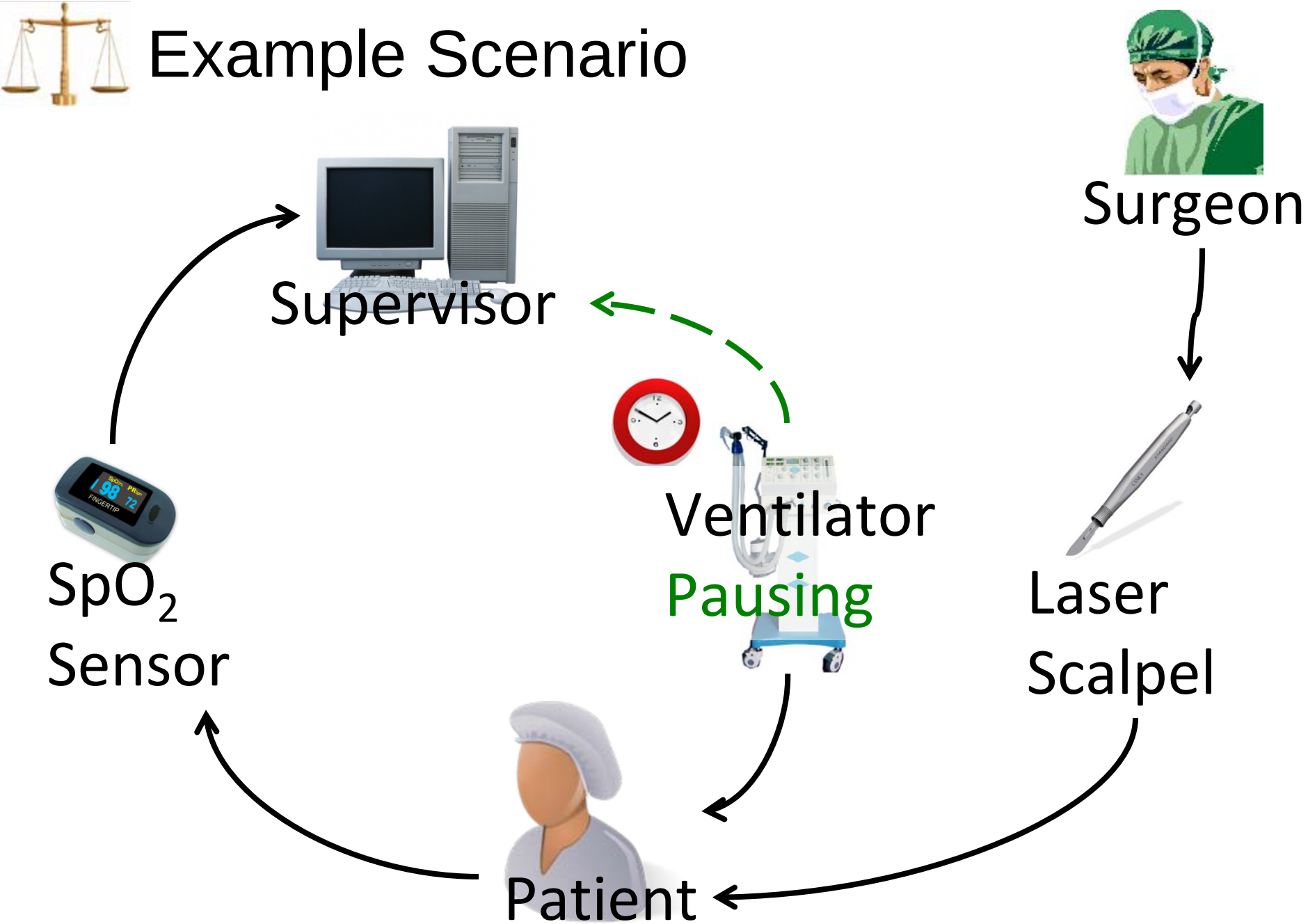
Example Scenario



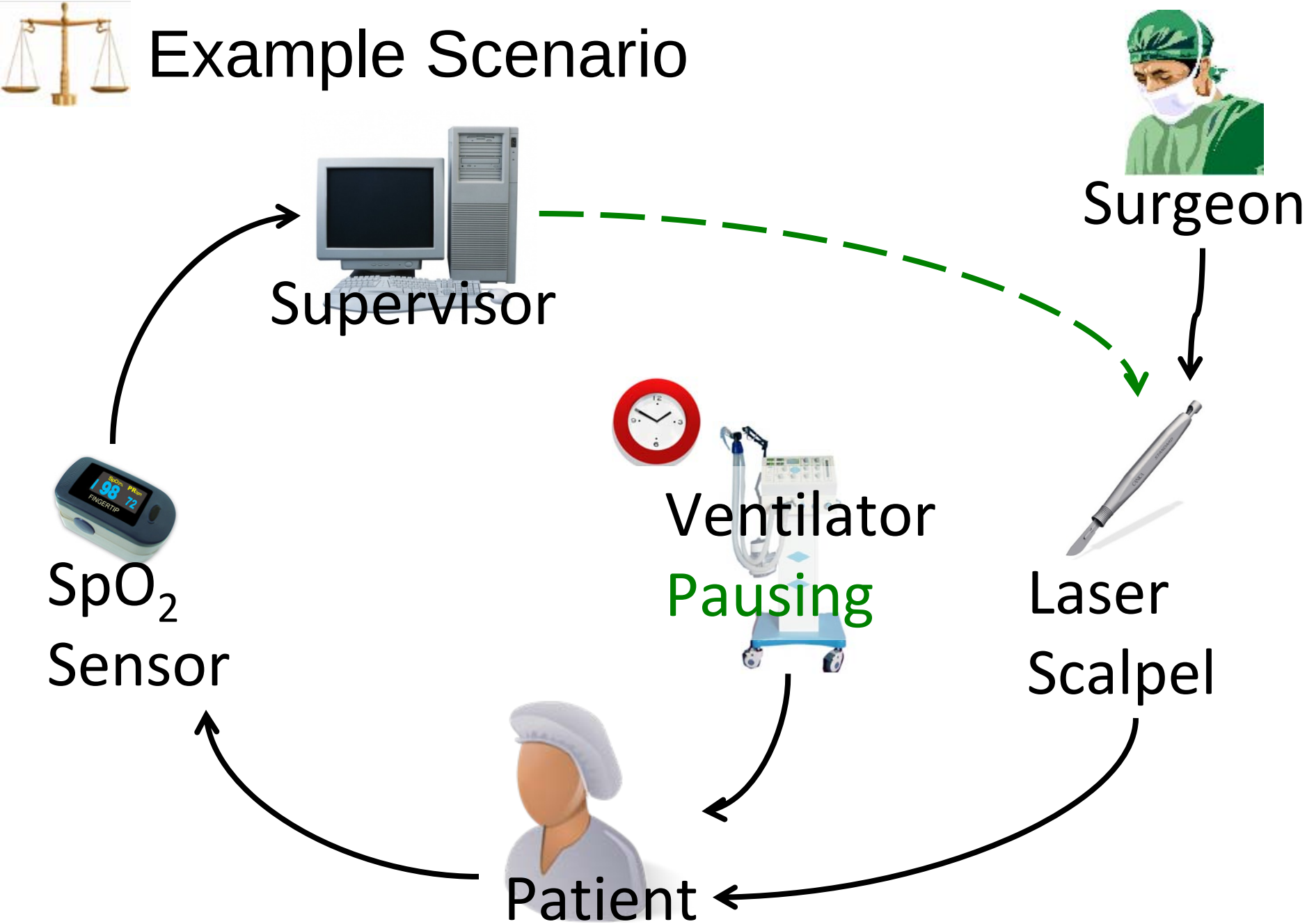
Example Scenario



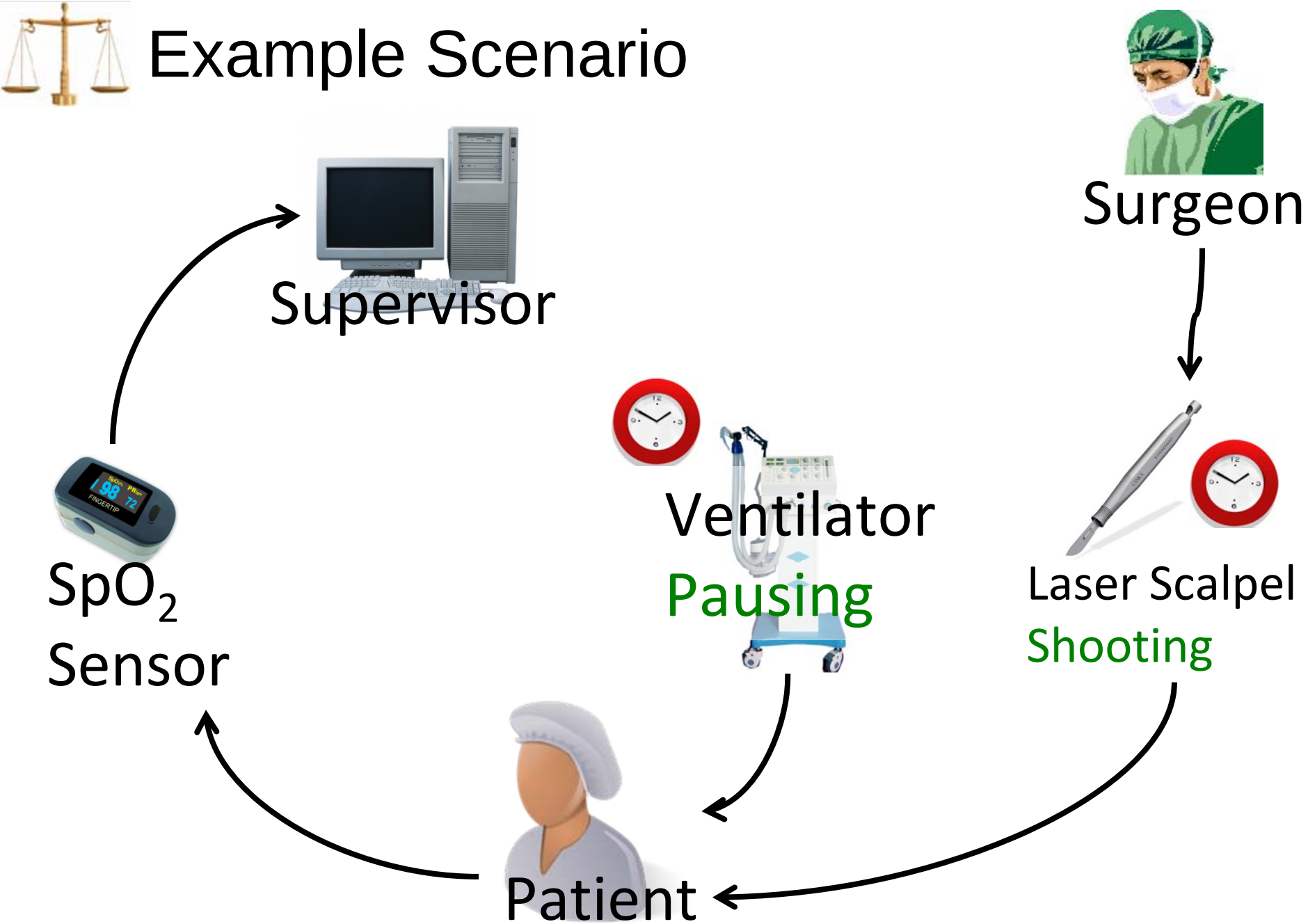
Example Scenario



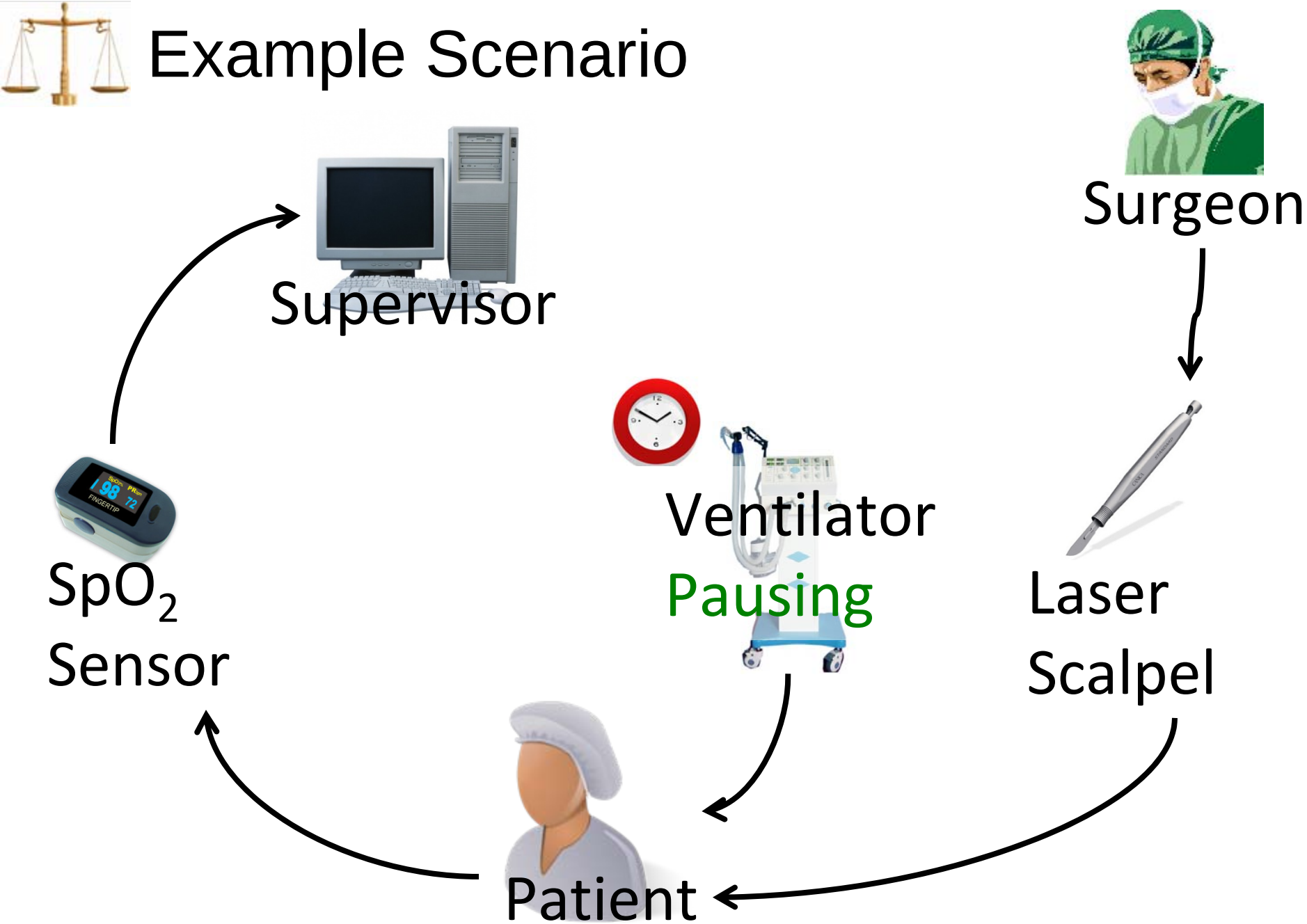
Example Scenario



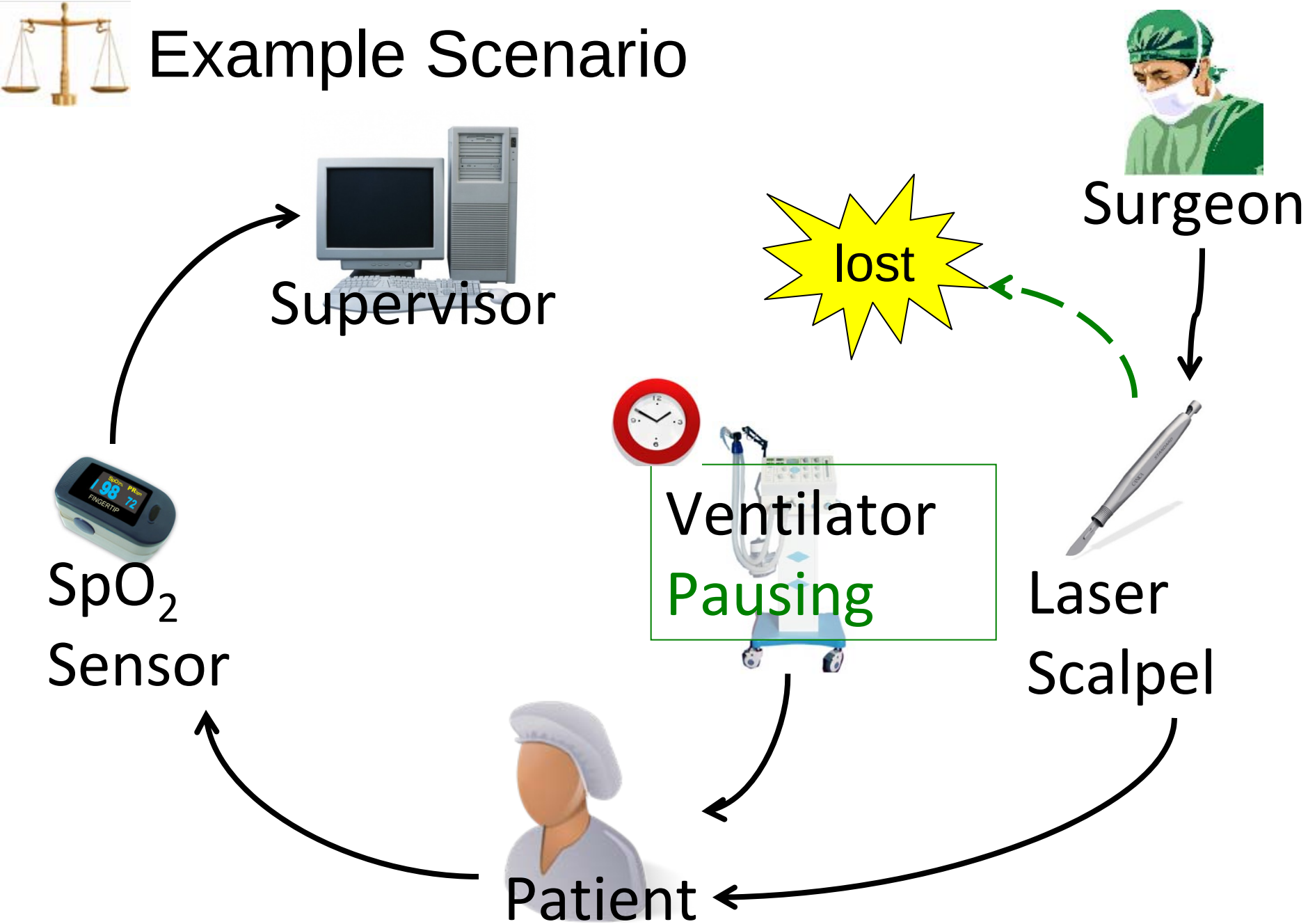
Example Scenario



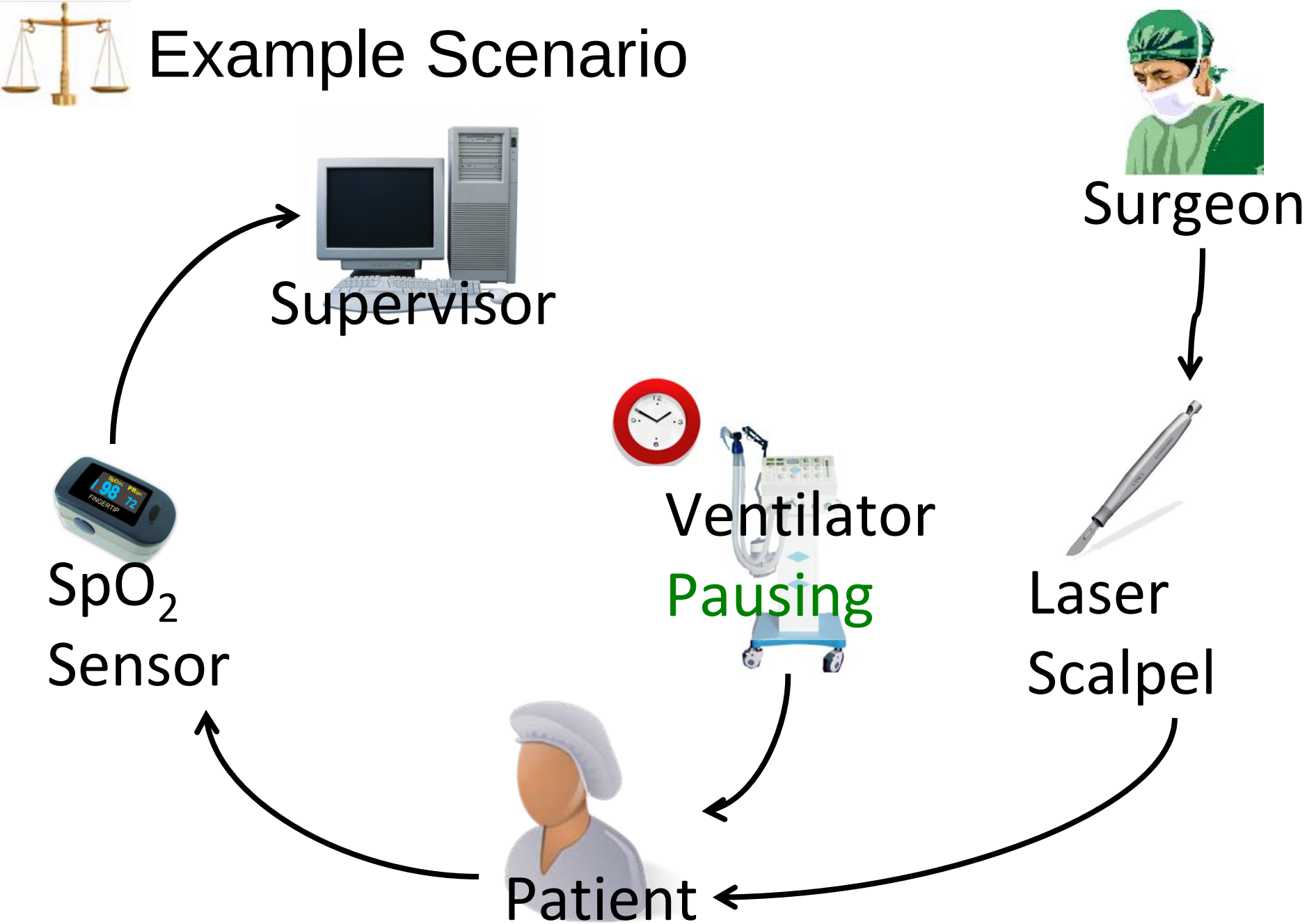
Example Scenario



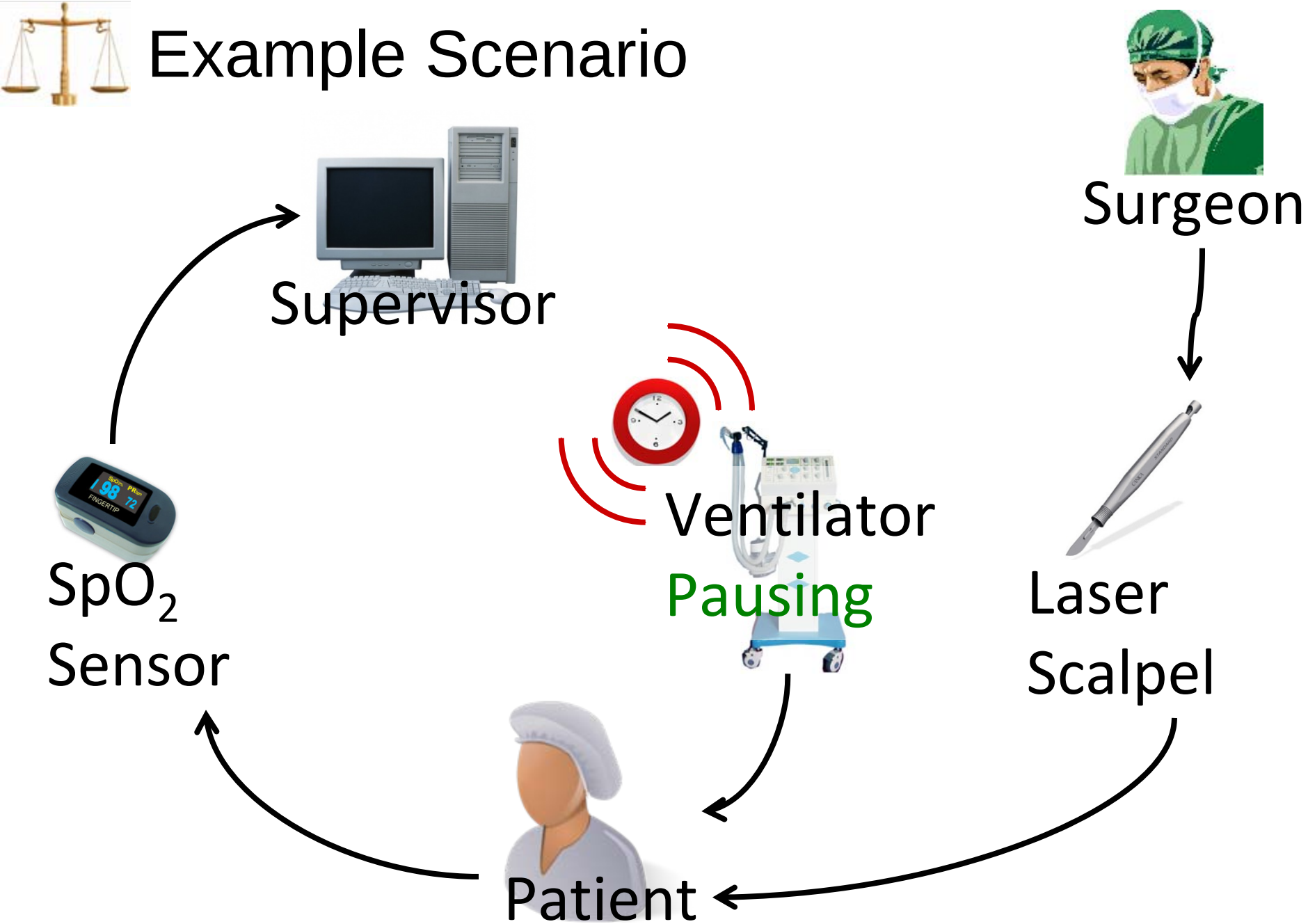
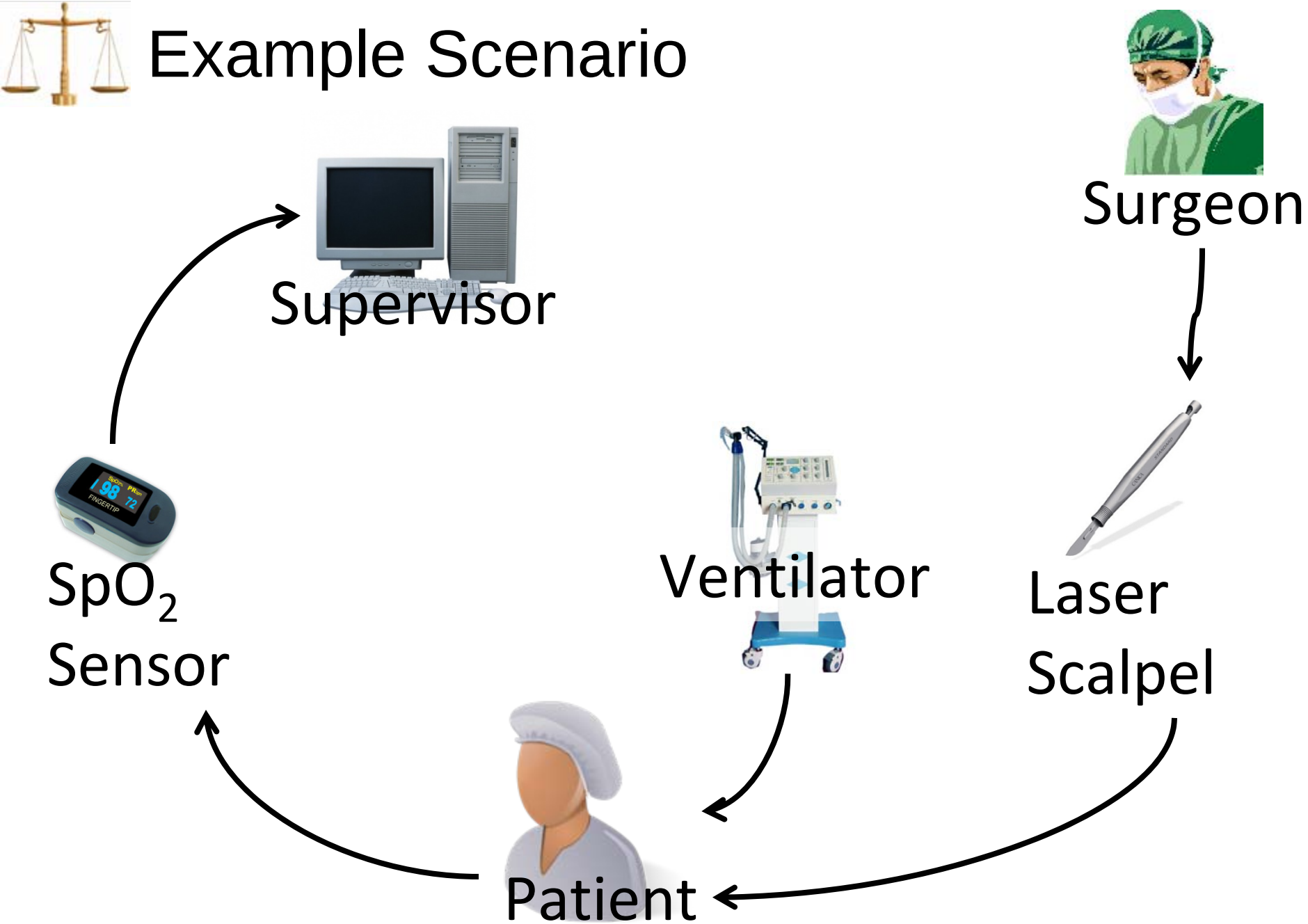
Example Scenario



Example Scenario



Example Scenario



Example Scenario