Synchronization and Communication (part II)

Real-Time Systems, Lecture 4

Martina Maggio

24 January 2017

Lund University, Department of Automatic Control
`www.control.lth.se/course/FRTN01`

Content

[Real-Time Control System: Chapter 4]

1. Deadlock
2. Priority Inversion
3. Message Passing

Deadlock

Deadlock

Improper allocation of common resources may cause deadlocks.

Example: A and B both need access to two common resources, protected by the semaphores R1 and R2 (initialized to 1). May cause deadlock.

Process A	Process B
`...`	`...`
`wait(R1);`	`wait(R2);`
`wait(R2);`	`wait(R1);`
`...`	`...`
`signal(R2);`	`signal(R1);`
`signal(R1);`	`signal(R2);`
`...`	`...`

Deadlock Handling

- Deadlock Prevention:
  - e.g., hierarchical resource allocation.
- Deadlock Avoidance (at runtime):
  - e.g., priority ceiling protocol.
- Deadlock Detection and Recovery (at runtime):
  - e.g., using model checking.

Deadlock: Necessary Conditions

Conditions that must happen for a deadlock to occurr:

1. *Mutual exclusion:* only a bounded number of processes can use a resource at a time;
2. *Hold and wait:* processes must exist which are holding resources while waiting for other resources;
3. *No preemption:* resources can only be released voluntarily by a process;
4. *Circular wait:* a circular chain of processes must exist such that each process holds a resource that is requested by the next process in the chain.

Deadlock Prevention

To prevent deadlock it is possible to remove one of the four conditions:

1. *Mutual exclusion* – usually unrealistic;
2. *Hold and wait* – require that the processes preallocate all resources before execution or at points when they have no other resources allocated;
3. *No preemption* – forced resource deallocation;
4. *Circular wait* – ensure that resources always are allocated in a fixed order.

Hierarchical Resource Allocation

Pyramidal resource allocation. A resource belongs to one of the classes R_i where $i = 1 \ldots n$. A process must reserve resources following the classes order. If it has a resource of order m it cannot reserve a resource of order p where $p < m$.

Process A

```
...
wait(R1);
wait(R2);
...
signal(R2);
signal(R1);
...
```

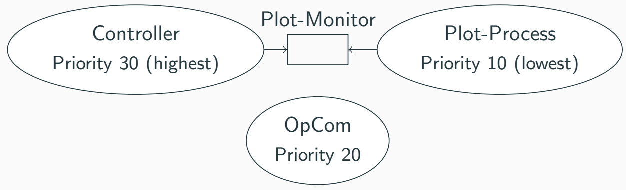
Process B

```
...
wait(R1);
wait(R2);
...
signal(R2);
signal(R1);
...
```


Priority Inversion

Priority Inversion

Priority inversion can happen when a high-priority process becomes blocked by a lower priority process and there is no common resource involved between the two processes.



(1) Plot-Process enters Plot-Monitor; (2) an interrupt cause OpCom to execute; (3) an interrupt cause Controller to execute; (4) Controller tries to enter Plot-Monitor and is blocked, because the monitor is held by Plot-Process, but Plot-Process cannot execute because OpCom has higher priority. **OpCom is blocking Controller.**

Priority Inversion

Solutions:

- Priority Inheritance;
- Priority Ceiling Protocol;
- Immediate Inheritance.

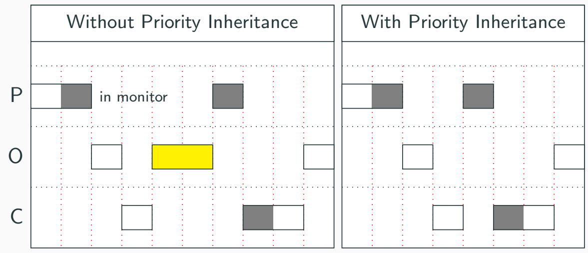
Priority Inheritance

During the execution of `Enter`, if the monitor is occupied then the priority of the process holding the monitor is raised to the priority of the process that called `Enter`. The priority is reset when the process holding the monitor calls `Leave`. This is for example how the problem is solved in STORK.

In the example, when Controller tries to enter Plot-Monitor, the priority of Plot-Process is raised to 30 (highest), there is a context switch to Plot-Process and as soon as Plot-Process relases the lock, there is a context switch to Controller. When Controller releases the CPU, OpCom can be executed.

Priority Inheritance

P: Plot-Process; O: OpCom; C: Controller.



Example: Mars Pathfinder 1997

After a while the spacecraft experienced total system resets, resulting in losses of meteorological data. Reason:

- a mutex-protected shared memory area for passing information;
- a high priority bus management task, frequently passing data in/out;
- an infrequent data gathering task at low priority, entering data into the memory;
- a third communication task at medium priority, not accessing the shared memory;
- occasionally, the situation arised where the mutex was held by the low priority task, the high priority task was blocked on the mutex, and the medium priority task was executing, preventing the low priority task from leaving the mutex.

Classical Priority Inversion Situation

Example: Solution

- VxWorks from Wind River Systems;
- binary mutex semaphores with an optional initialization argument that decides if priority inheritance should be used or not;
- upload of code that modified the symbol tables of the Pathfinder so that priority inheritance was used.

The Priority Ceiling Protocol

L. Sha, R. Rajkumar, J. Lehoczky, Priority Inheritance Protocols: An Approach to Real-Time Synchronization, IEEE Transactions on Computers, Vol. 39, No. 9, 1990

Restrictions on how we can lock (Wait, EnterMonitor) and unlock (Signal, LeaveMonitor) resources:

- a task must release all resources between invocations;
- the computation time that a task i needs while holding semaphore s is bounded. $cs_{i,s}$ = the time length of the critical section for task i holding semaphore s;
- a task may only lock semaphores from a fixed set of semaphores known a priory. $uses(i)$ = the set of semaphores that may be used by task i.

The Priority Ceiling Protocol

The *ceiling* of a semaphore, $ceil(s)$, is the priority of the highest priority task that uses the semaphore; $pri(i)$ is the priority of task i. During run-time:

- if a task i wants to lock a semaphore s, it can only do so if $pri(i)$ is **strictly higher** than the ceilings of all semaphores currently locked by **other** tasks;
- if not, task i will be blocked (task i is said to be blocked on the semaphore, S^*, with the highest priority ceiling of all semaphores currently locked by other jobs and task i is said to be blocked by the task that holds S^*);
- when task i is blocked on S^*, the task currently holding S^* inherits the priority of task i.

The Priority Ceiling Protocol

Properties:

- deadlock free;
- a given task i is delayed at most once by a lower priority task;
- the delay is a function of the time taken to execute the critical section.

The Priority Ceiling Protocol

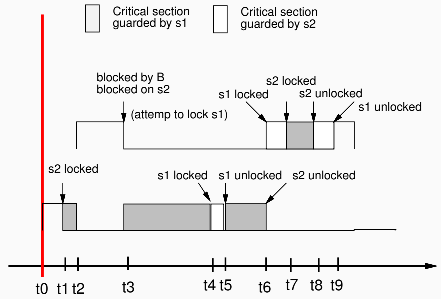
- Task A: priority 10 — Task B: priority 9

```
Task A
...
lock(s1);
lock(s2);
...
unlock(s1);
unlock(s2);
...
```

```
Task B
...
lock(s2);
lock(s1);
...
unlock(s1);
unlock(s2);
...
```

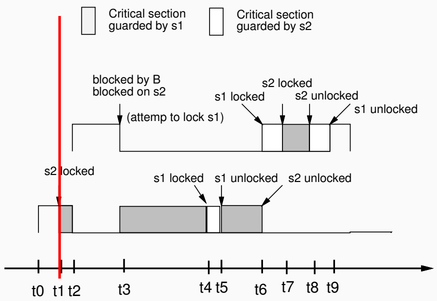
- $ceil(s_1) = 10$ — $ceil(s_2) = 10$

The Priority Ceiling Protocol



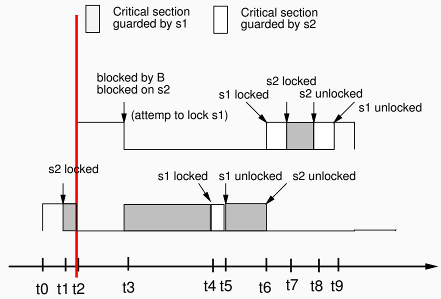
t_0: B starts executing.

The Priority Ceiling Protocol



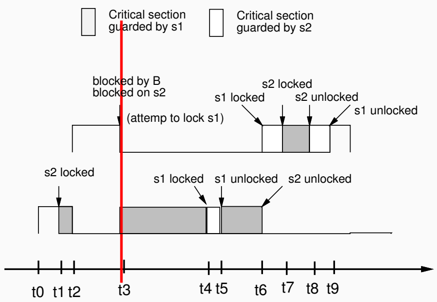
t_1: B attempts to lock s_2, it succeeds since no lock is held by another task.

The Priority Ceiling Protocol



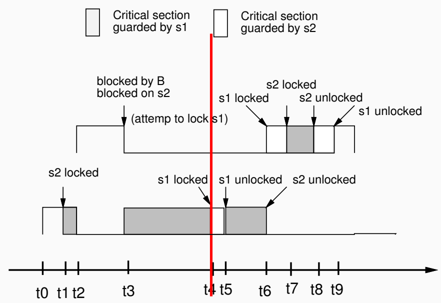
t_2: A preempts B.

The Priority Ceiling Protocol



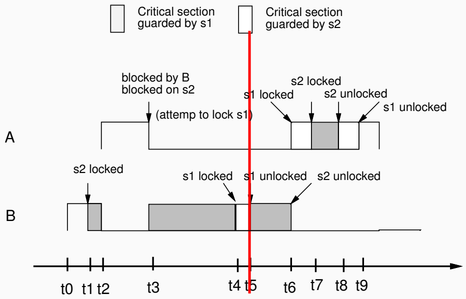
t_3: A tries to lock s_1 and fails since A's priority (10) is not stricly higher than the ceiling of s_2 (10) that is held by B. A is blocked by B on s_2. The priority of B is raised to 10.

The Priority Ceiling Protocol



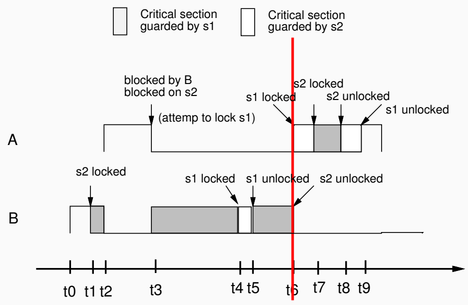
t_4: B attempts to lock s_1. It succeeds since there are no locks held by any other task.

The Priority Ceiling Protocol



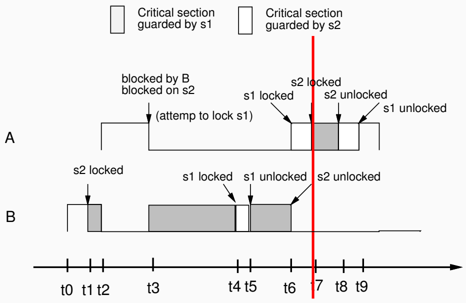
t_5: B unlocks s_1.

The Priority Ceiling Protocol



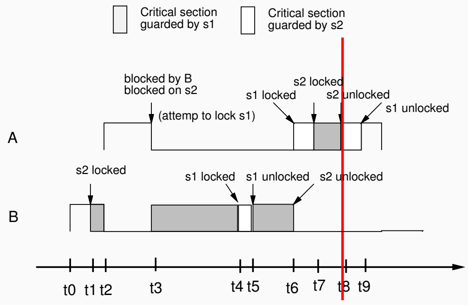
t_6: B unlocks s_2. The priority of B is lowered to the original priority (9), A preempts B, attempts to lock s_1 and succeeds.

The Priority Ceiling Protocol



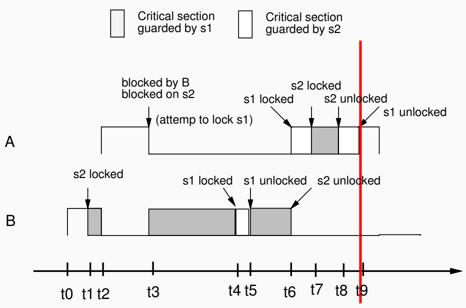
t_7: A attempts to lock s_2 and succeeds.

The Priority Ceiling Protocol



t_8: A unlocks s_2.

The Priority Ceiling Protocol



t_8: A unlocks s_1.

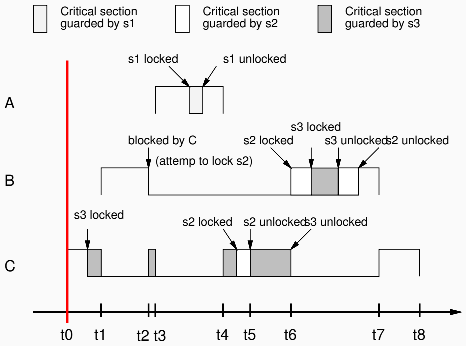
The Priority Ceiling Protocol

- Task A: priority 10 — Task B: priority 9 — Task C: priority 8

Task A	**Task B**	**Task C**
`...`	`lock(s2);`	`lock(s3);`
`lock(s1);`	`...`	`...`
`...`	`lock(s3);`	`lock(s2);`
`unlock(s1);`	`...`	`...`
`...`	`unlock(s3);`	`unlock(s2);`
`...`	`...`	`...`
`...`	`unlock(s2);`	`unlock(s3);`

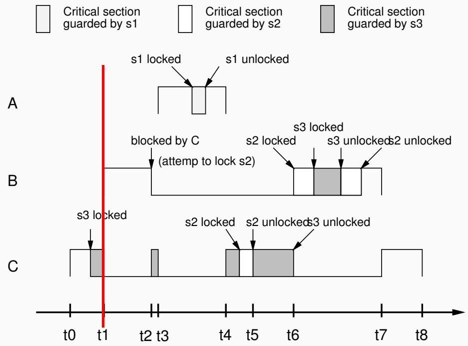
- $ceil(s_1) = 10$ — $ceil(s_2) = 9$ — $ceil(s_3) = 9$

The Priority Ceiling Protocol



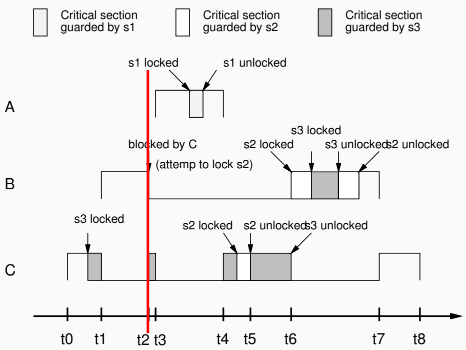
t_0: C starts executing and locks s_3.

The Priority Ceiling Protocol



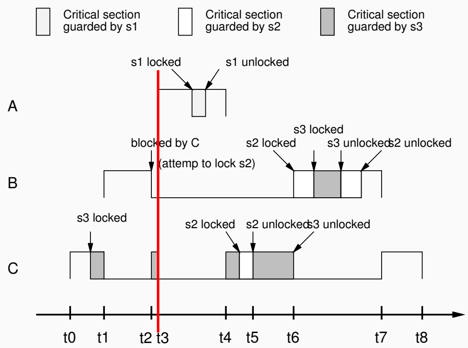
t_1: B preempts C.

The Priority Ceiling Protocol



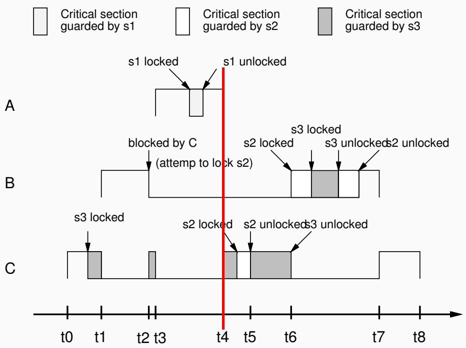
t_2: B tries to lock s_2 and fails. The priority of B (9) is not strictly higher than the ceiling of s_3 (9) that is held by C. B blocks on s_3 (which means that B is blocked by C). C inherits the priority of B (9).

The Priority Ceiling Protocol



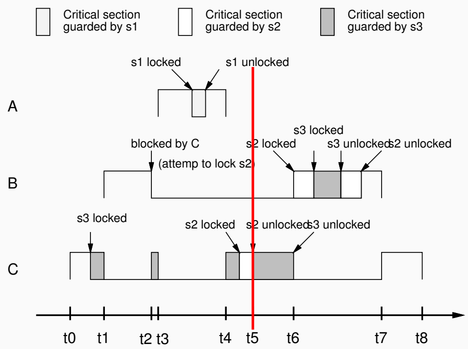
t_3: A preempts C and tries to lock s_1 and succeeds. The priority of A (10) is higher than the ceiling of s_3, which is locked (9).

The Priority Ceiling Protocol



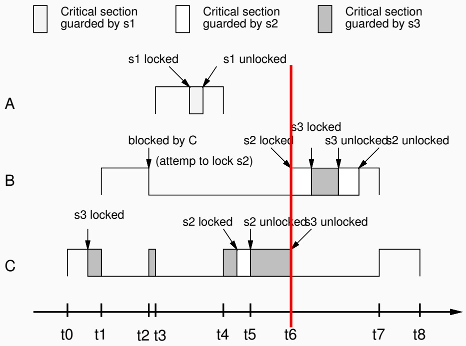
t_4: A completes. C resumes and tries to lock s_2 and succeeds (C itself is the holder of the lock on s_3.

The Priority Ceiling Protocol



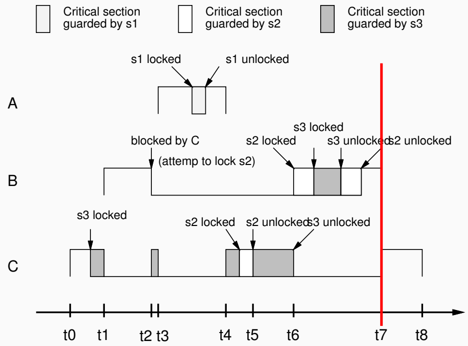
t_5: C unlocks s_2.

The Priority Ceiling Protocol



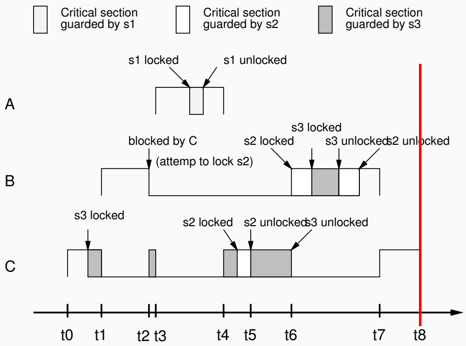
t_6: C unlocks s_3 and gets back his basic priority (8). B preempts C and attempts to lock s_2 and succeeds. Then B locks s_3 and unlocks s_3 and s_2.

The Priority Ceiling Protocol



t_7: B completes and C is resumed.

The Priority Ceiling Protocol



t_8: C completes.

The Priority Ceiling Protocol

- A is never blocked;
- B is blocked by C during the intervals $[t_2, t_3]$ and $[t_4, t_6]$. However, B is blocked for no more than the duration of one time critical section of the lower priority task C even though the actual blocking occurs over disjoint time intervals.

The Priority Ceiling Protocol

General Properties:

- with ordinary priority inheritance, a task i can be blocked for at most the duration of $\min(n, m)$ critical sections, where n is the number of lower priority tasks that could block i and m is the number of semaphores that can be used to block i;
- with the priority ceiling inheritance, a task i can be blocked for at most the duration of one longest critical section;
- sometimes priority ceiling introduces unnecessary blocking but the worst-case blocking delay is much less than for ordinary priority inheritance.

The Immediate Inheritance Protocol

- When a task obtains a lock the priority of the task is immediately raised to the ceiling of the lock;
- the same worst-case timing behavior as the priority ceiling protocol;
- easy to implement;
- on a single-processor system it is not necessary to have any queues of blocked tasks for the locks (semaphores, monitors) – tasks waiting to acquire the locks will have lower priority than the task holding the lock and can, therefore be queued in `ReadyQueue`;
- also known as the Priority Ceiling Emulation Protocol or the Priority Protect Protocol.

[JAVA] Priority Inheritance

Priority inheritance is a common, but not mandatory, feature of most Java implementations.

The Real-Time Java Specification requires that the priority inheritance protocol is implemented by default. The priority ceiling protocol is optional.

Message Passing

Mailbox Communication

A process/thread communicates with another process/thread by sending a message to it.

Synchronization models:

- **Asynchronous:** the sender process proceeds immediately after having sent a message. Requires buffer space for sent but unread messages. Used in the course.
- **Synchronous:** the sender proceeds only when the message has been received. Rendez-vous.
- **Remote Invocation:** the sender proceeds only when a reply has been received from the receiver process. Extended rendez-vous. Remote Procedure/Method Call (RPC/RMC).

Naming Schemes

- **Direct naming**:
  `send "message" to "process"`
- **Indirect naming**:
  `send "message" to "mailbox"`

With indirect naming different structures are possible:
(*) many to one, (*) many to many, (*) one to one, (*) one to many.

Message Types

- System- or user-defined data structures;
- The same representation at the sender and at the receiver;
- Shared address space (pointer, copy data).

Message Buffering

Asynchronous message passing requires buffering.

The buffer size is always bounded.

A process is blocked if it tries to send to a full mailbox.

Problematic for high-priority processes.

The message passing system must provide a primitive that only sends a message if the mailbox has enough space.

Similarly, the message passing system must provide a primitive that makes it possible for a receiver process to test if there is a message in the mailbox before it reads.

[JAVA] Message Passing

The `se.lth.cs.realtime.event` package provides support for mailboxes:

- asynchronous message passing;
- both direct naming and indirect naming can be implemented.

However, in most examples one assumes that each thread (e.g., a consumer threads) contains a mailbox for incoming messages.

[JAVA] Messages

Messages are implemented as instances of objects that are subclasses to `RTEvent`. Messages are always time-stamped.

Constructors:

- `RTEvent()`: Creates an RTEvent object with the current thread as source and a time-stamp from the current system time;
- `RTEvent(long ts)`: Creates an RTEvent object with the current thread as source and with the specified time stamp.
- `RTEvent(java.lang.Object source)`: Creates an RTEvent object with the specified source object and a time-stamp from the current system time.
- `RTEvent(java.lang.Object source, long ts)`: Creates an RTEvent object with the specified source object and time stamp.

[JAVA] Messages

A time-stamp supplied to the constructor may denote the time when input was sampled, rather than when an output event was created from a control block or digital filter.

The source is by default the current thread, but a supplied source may denote some passive object like a control block run by an external thread.

[JAVA] Messages

Methods:

- `getSource()`: returns the source object of the RTEvent;
- `getTicks()`: returns the event's time stamp in number of system-dependent ticks;
- `getSeconds()`: returns the timestamp in seconds;
- `getMillis()`: returns the timestamp in milliseconds.

[JAVA] Mailboxes

Mailboxes (message buffers) implemented by the class `RTEventBuffer`. Synchronized bounded buffer with both blocking and non-blocking methods for sending (posting) and reading (fetching) messages. The class attributes are declared `protected` in order to make it possible to create subclasses with different behavior.

Constructor:

- `RTEventBuffer(int maxSize)`

[JAVA] Mailboxes

Methods:

- `doPost(RTEvent e)`: adds an RTEvent to the queue, blocks caller if the queue is full;
- `tryPost(RTEvent e)`: Adds an RTEvent to the queue, without blocking if the queue is full; returns null if the buffer is non-full, the event e otherwise;
- `doFetch()`: returns the next RTEvent in the queue, blocks if none available;
- `tryFetch()`: returns the next available RTEvent in the queue, or null if the queue is empty;
- `awaitEmpty()`: waits for buffer to become empty;
- `awaitFull()`: waits for buffer to become full;
- `isEmpty()`: checks if buffer is empty;
- `isFull()`: checks if buffer is full.

[JAVA] Producer-Consumer

```java
class Producer extends Thread {
  Consumer receiver;
  MyMessage msg;

  public Producer(Consumer theReceiver) {
    receiver = theReceiver;
  }

  public void run() {
    while (true) {
      char c = getChar();
      msg = new MyMessage(c);
      receiver.putEvent(msg);
    }
  }
}
```


[JAVA] Producer-Consumer

```java
class Consumer extends Thread {
  private RTEventBuffer inbox;

  public Consumer(int size) { inbox = new RTEventBuffer(size); }
  public void putEvent(MyMessage msg) { inbox.doPost(msg); }

  public void run() {
    RTEvent m;
    while (true) {
      m = inbox.doFetch();
      if (m instanceof MyMessage) {
        MyMessage msg = (MyMessage) m ;
        useChar(msg.ch);
      } else {
        // Handle other messages
      };
    }
  }
}
```


Message Passing: add-ons

- **Selective waiting**: a process is only willing to accept messages of a certain category from a mailbox or directly from a set of processes (like Ada).
- **Time out**: time out on receiver processes.
- **Priority-sorted mailboxes**: urgent messages have priority over non-urgent messages.

[LINUX] Mailboxes

Mailbox communication is supported in a number of ways in Linux. One possibility is to use pipes, named pipes (FIFOs), or sockets, directly.

Another possibility is POSIX Message Passing. Very similar in functionality to the Mailbox system already presented.

Several other alternatives, like D-Bus `http://www.freedesktop.org/wiki/Software/dbus`

Message Passing (summary)

Can be used both for communication and synchronization.

Using empty messages a mailbox corresponds to a semaphore.

Well suited for distributed systems.

Passing objects through a buffer

```java
public class Buffer {
  private Object data;
  private boolean full = false;
  private boolean empty = true;

  public synchronized void put(Object inData) {
    while (full) {
      try {
        wait();
      } catch (InterruptedException e) { e.printStackTrace(); }
    }
    data = inData;
    full = true;
    empty = false;
    notifyAll();
  }
```

Passing objects through a buffer

```java
  public synchronized Object get() {
    while (empty) {
      try {
        wait();
      } catch (InterruptedException e) { e.printStackTrace(); }
    }
    full = false;
    empty = true;
    notifyAll();
    return data;
  }
}
```


Passing objects through a buffer

Sender Thread:

```java
public void run() {
  Object data = new Object();
  while (true) {
    // Generate data
    b.put(data);
  }
}
```

Receiver Thread:

```java
public void run() {
  Object data;
  while (true) {
    data = b.get();
    // Use data
  }
}
```


Passing objects through a buffer

Very dangerous. The object reference in the receiver thread points at the same object as the object reference in the sender thread. All modifications will be done without protection.

Approach 1: New objects

```java
public void run() {
  Object data = new Object();
  while (true) {
    // Generate data
    b.put(data);
    data = new Object();
  }
}
```


Passing objects through a buffer

Approach 2: Copying in the buffer

```java
public synchronized void put(Object inData) {
  while (full) {
    try {
      wait();
    } catch (InterruptedException e) { e.printStackTrace(); }
  }
  data = inData.clone(); // generate a copy of the data
  full = true;
  empty = false;
  notifyAll();
}
```


Passing objects through a buffer

Approach 3: Immutable objects

- An immutable object is an object that cannot be modified once it has been created.
- An object is immutable if all data attributes are declared private and no methods are declared that may set new values to the data attributes.
- The sender sends immutable objects. It is not possible for the user to modify them in any dangerous way.