# Distributed Systems Programming (F2.9NM1)

*LOTOS Assignment*

The Absolute Block System of Railway Signalling:

An Exercise in the Specification of a Distributed Concurrent System

Andrew Ireland

## 1 Introduction

The *Absolute Block System* (ABS) of railway signalling was developed in Britain during the $19^{th}$ century and refined during the first half of the $20^{th}$ century [1, 2]. Although largely superseded[1] by fully electronic systems, ABS represents an interesting case study in the modelling of a distributed concurrent system. The aim of this assignment is to develop a specification of ABS in LOTOS using LOLA.

Background material on the operation of railways and ABS is presented in §2. The basis for a LOTOS specification of ABS is presented in §3. In §4 the actual specification task you are to undertake is described. This task involves you extending the specification given in §3. Finally, in §5 the basic structure of your assignment submission is detailed. Note that the required submission includes both a hard-copy and an e-mail component.

## 2 Background: The Absolute Block System

Most railways operate what is known as *double line working*, that is, railway lines run in parallel and each line carries trains in a particular direction. In normal working this arrangement eliminates the potential for head-on collisions. However, additional constraints are required in order to prevent other kinds of accidents, *e.g.* one train running into the rear of another which has broken down. ABS is a signalling system which aims to prevent such accidents. In the following sections we describe the structure and operation of ABS in detail.

### 2.1 The Block Section

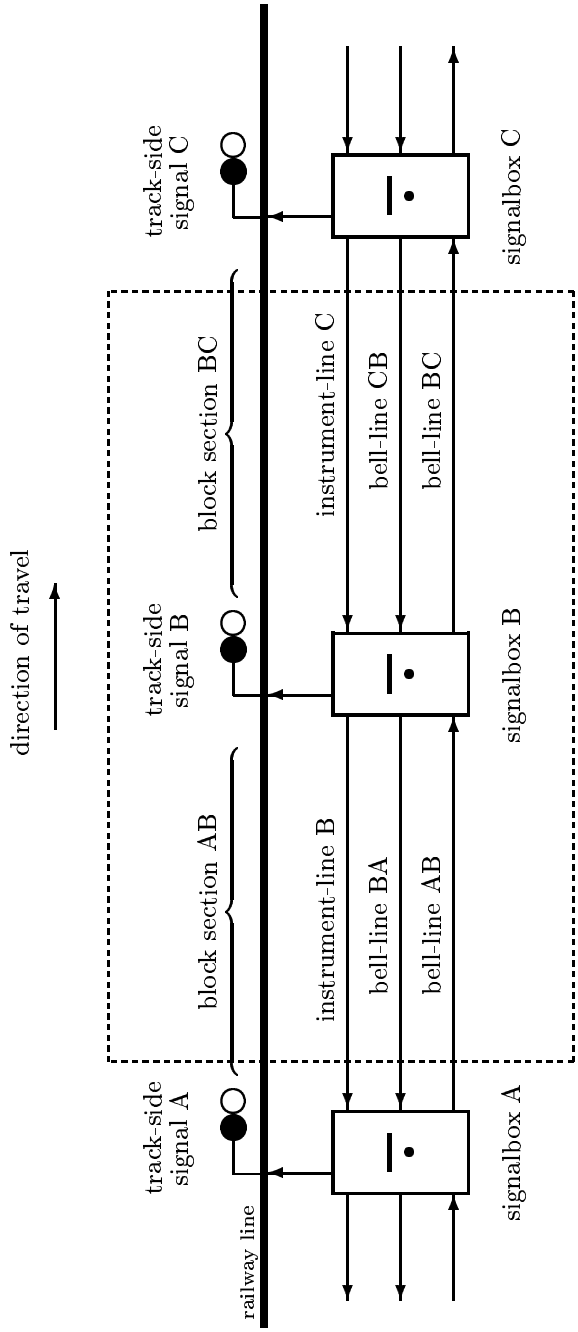
Within ABS railway lines are divided into a series of *block sections*. The aim of ABS is to ensure that only one train occupies the same line within a block section at the same time. ABS achieves this aim by positioning a *signalbox* between each block section. A signalbox has a human *operator*, the role of an operator is to work collaboratively with its neighbouring operators in order to control train access to the block sections. The equipment used to achieve this control is explained in the next section. In order to keep our explanation and your specification task relatively simple, we will consider a single[2] line railway where trains travel in one direction only. The basic layout of the railway network you are being asked to model is presented in figure 1.

### 2.2 Infrastructure: The Signalling Equipment

As mentioned above, signalboxes are located between block sections. In figure 1 signalbox B is said to be situated to *advance* of block section AB and to the *rear* of the block section BC.

[1] However, many railway networks throughout Britain still rely upon ABS.

[2] On double line working a block section is divided into two parts, *i.e.* the *up line* and the *down line*.




A single line railway is presented where trains travel in a fixed direction, *i.e.* left-to-right. The line is divided into a series of block sections, two block sections are explicitly named, *i.e.* AB and BC. Note that signalboxes are positioned between each block section. Three signalboxes are shown, A, B and C. Each signalbox controls a track-side signal that is used to regulate the entry of trains into the block section in advance of the signalbox's position. Note that signalboxes are linked by three lines of communication in either direction, *i.e.* a block and two bell instrument lines. Finally, the dashed box indicates the limits of the system that you are being asked to model using LOTOS.

Figure 1: A Single Line Railway

A signalbox operator at the rear of a block section controls train access to the block section via their track-side signal (see figure 1). A track-side signal has two settings:

- `danger`: indicating that a train should stop and wait;
- `clear`: indicating that a train should proceed into the next block section.

When dealing with trains which wish to enter a block section the operator at the rear is said to be acting in *forwarding mode* while the operator who is in advance is said to be acting in *accepting mode*. The operator who is acting in accepting mode has ultimate control over a train wishing to enter a block section, as will be explained in §2.3.

Each mode of operation makes use of a device called a *block instrument*. There are two types of block instrument, a *forwarding block instrument* and an *accepting block instrument* (see figure 2). Each signalbox contains both types of block instrument. A block instrument is used to record the status of a railway line within a particular block section. There are three distinct status settings associated with a block instrument:

- `line_blocked`: there is no train on the line;
- `line_clear`: the line is clear to accept a train;
- `train_on_line`: the line occupied.

For a given block section the signalbox in advance contains an accepting block instrument while the signalbox to the rear contains a forwarding block instrument. The status settings are selected by a control handle attached to the accepting block instrument and are automatically relayed to an associated forwarding block instrument. Note that the forwarding instrument simply repeats the settings which are displayed on the associated accepting instrument.

In addition to the block instruments, signalboxes are also connected by a *block bell* instrument (see figure 2) which enables neighbouring signalbox operators to communicate using bell signals. A greatly simplified version of the bell signals are given in table 1.

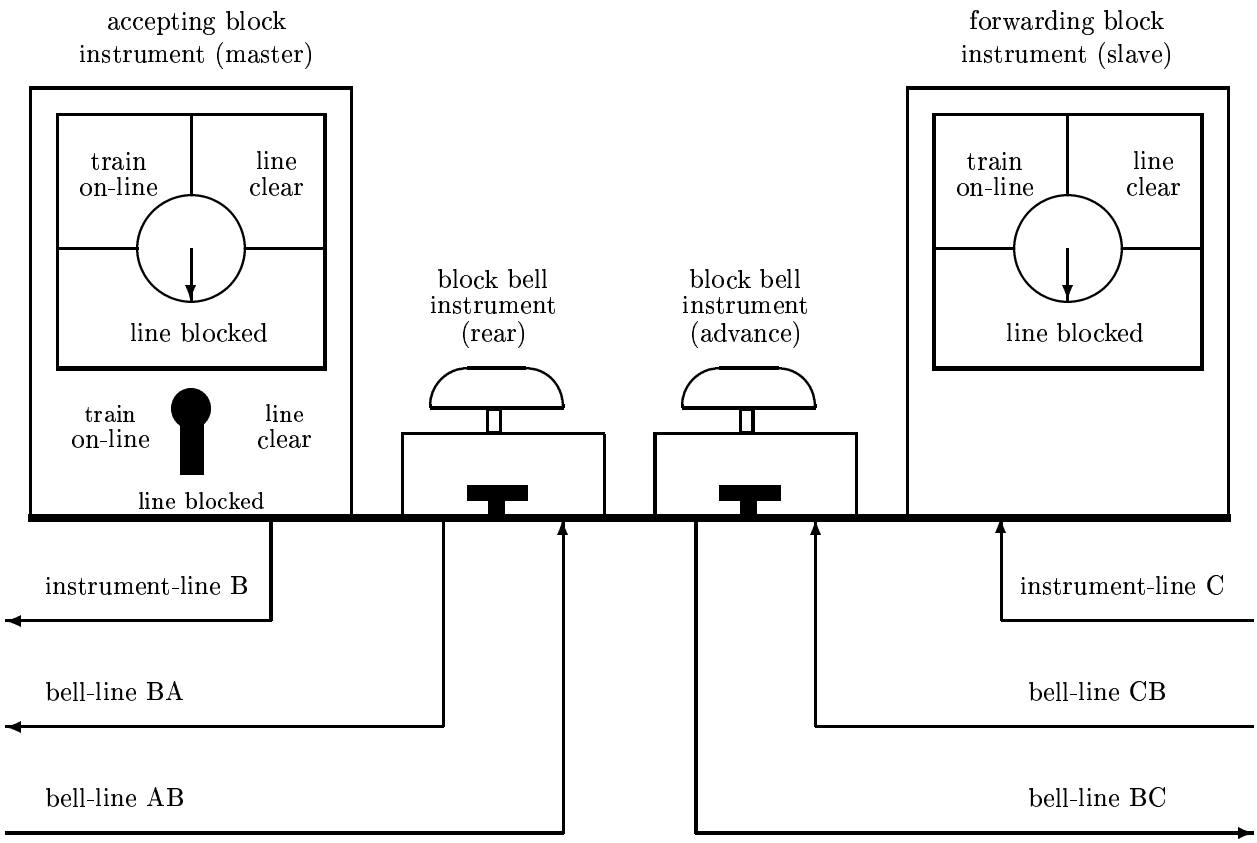
| **Meaning** | **No. beats** | **Sequence** |
|---|---|---|
| call attention | 1 | 1 |
| is line clear for a train | 4 | 3 pause 1 |
| train entering section | 2 | 2 |
| train out of section | 3 | 2 pause 1 |

Table 1: Block Bell Signals

## 2.3 Protocol: The Signalling Method

The signalbox operators control access to a block section. The method of control is described in detail below. Our description relates to figure 1 where three signalboxes, A, B and C, are shown. The method of control is illustrated in terms of a train travelling from A to B and then onto C.

We focus firstly on a trains journey from A to B. In order for a train to pass from A to B it must pass through the block section AB. To achieve this, A and B will work in forwarding and accepting modes respectively. A begins by sending B the "call attention" bell signal — 1 bell beat (see table 1 for a description of the bell signals). B must acknowledge A's signal by repeating the "call attention" bell signal. On hearing this acknowledgement A then sends the "is line clear for a train" bell signal to B. If B can accept the train being offered, *i.e.* line within the block section AB is unoccupied, then B acknowledges A's request by repeating the "is line clear for a train" bell signal and sets their accepting block instrument to `line_clear`. Once A hears the acknowledgement and sees the `line_clear` setting relayed on their forwarding block instrument then they set their track-side signal to `clear` and send the "train entering section" bell signal to B. On receiving the "train entering section" signal B must repeat it back to A and then set their accepting block instrument to `train_on_line`. Once the train enters the block section AB, A should return their track-side signal to `danger`, this prevents a following train entering the block section. Once a train has exited block




Shown above are the instruments located within each signalbox which provide the only means of communication with neighboring signalboxes. Because the assignment requires you to model signalbox B, we have labelled the instrument and bell lines accordingly. Note that **only** the **accepting block instrument** has a control handle. This is because the **forwarding block instrument** has no control over its associated status pointer, it simply repeats the setting of the status pointer on the **accepting block instrument** within signalbox C.

Figure 2: Signalbox Communication Instruments

section AB and has passed B's track-side signal, *i.e.* entered block section BC, then B must return their track-side signal to `danger` and send the "call attention" bell signal to A. A must acknowledge B's signal by repeating it as before. After B receives an acknowledgement it sends the "train out of section" bell signal to A and then sets their accepting block instrument to `line_blocked`. Note that until block section AB is classified as `line_blocked` then B **should not** accept any more trains from A.

The passage of a train from B to C follows the same pattern as describe above for the passage of a train from A to B. Note, however, that in the context of a train travelling from B to C, it is B who acts in forwarding mode while C acts in accepting mode.

# 3 A Specification of the Block Section

A LOTOS specification of a block section is presented in figure 3. We use a process called `BLK_SEC` to represent the notion of a block section. The process has two associated actions, *i.e.* `enterBS` and `exitBS`. The first action models a train's entry into the block section while the second action models a trains departure from the block section. Recall from §2.1 that the basic safety property we are interested in is:

> *"... only one train occupies the same railway line within a block section at the same time."*

One way of checking whether or not this property is achieved is to simply keep a count of the number of trains which are in a blocked section any point in time. This is achieved in our definition of `BLK_SEC` by including a parameter called `count` which is incremented whenever the `enterBS` action occurs and which is decremented when the `exitBS` action occurs. Note that `BS` is always ready to synchronize on an `enterBS` action but will only synchronize on an `exitBS` action if `count` is greater than 0, *i.e.* there needs to be a train within the block section before one can depart.

# 4 The Specification Task

Your task is to extend the specification given in figure 3 so that it models ABS as described in §2. Your extended specification should include:

1. A process called `SIGNAL` which models the physical track-side signal. `SIGNAL` will record whether the track-side signal is displaying the `clear` or `danger` signal. The process `SIGNAL` provides the gateway between two instances of the `BLK_SEC` process, *i.e.* a `SIGNAL` process will interact with the `exitBS` action associated with one `BLK_SEC` process instance and the `enterBS` action of another `BS` process instance. Note that the `exitBS` and `enterBS` action sequence represents the movement of a train from one block section to the next block section. This action sequence should only take place if the associated track-side signal is displaying the `clear` signal;

2. A process called `BOX` which models the physical equipment within a signalbox as well as the actions which are performed by the signalbox operator. A `BOX` process will have to be able to:

   - Interact with the signalboxes to the rear and in advance of its own position through the block bell and block instruments;
   - Control its associated track-side signal through interaction with a `SIGNAL` process;
   - Observe when a train has entered the block section in advance of its position.

3. A composite behaviour which models the basic ABS. This should involve four process instances, *i.e.* two `BLK_SEC` processes, a `BOX` process and a `SIGNAL` process. You should specify the composite behaviour so that the interactions between the `BOX` and `SIGNAL` processes are unobservable. All processes **should be non-terminating**.

You should use LOLA to develop your specification. Relating the specification task to figure 1, you are being asked to model block sections AB and BC, the operations performed by signalbox B and its associated track-side signal. Signalboxes A and C are not part of the specification task, they

```
SPECIFICATION BLOCK_SECTION[enterBS, exitBS] : NOEXIT

LIBRARY Boolean ENDLIB

   TYPE Count IS Boolean
      SORTS count
      OPNS  0        :              -> count
            inc, dec : count        -> count
                _eq_ : count, count -> bool
            noi, nod : count        -> bool
      EQNS  FORALL x,y : count
            OFSORT count
              inc(dec(x))=x; dec(inc(x))=x;
            OFSORT bool
              nod(0) = true; nod(inc(x)) = nod(x);
              noi(0) = true; noi(dec(x)) = noi(x);
              0 eq 0 = true;
              inc(x) eq y = x eq dec(y);
              dec(x) eq y = x eq inc(y);
              nod(x) => 0 eq inc(x) = false;
              noi(x) => 0 eq dec(x) = false;
   ENDTYPE

BEHAVIOUR

BLK_SEC[enterBS, exitBS](0)

WHERE
   PROCESS BLK_SEC[enterBS, exitBS](trains:count) : NOEXIT :=

     (enterBS;
      BLK_SEC[enterBS, exitBS](inc(trains)))
                                            []
     ([not(trains eq 0)] -> exitBS;
                            BLK_SEC[enterBS, exitBS](dec(trains)))
   ENDPROC
ENDSPEC
```

A LOTOS specification of the *block section* is presented. Note that a counter is used in order to record the number of trains which occupy the block section at any given point in time. Note that the counter is initially set to 0, indicating that the block section is initially unoccupied. The source for the specification can be obtained via the following URL:

`http://www.cee.hw.ac.uk/~air/lotos/block_sec.lot`

Figure 3: A LOTOS Specification of the Block Section

represent the interface (or environment) to your specification. However, your specification should be constructed in a modular way so that any number of block sections and signalboxes can be added.

**Note that your specification will be evaluated in terms of its modularity and on how accurately you have modelled the real-world instruments and procedures associated with the ABS signalling protocol.**

In order to develop and test your specification you will need to simulate the context in which signalbox B operates using LOLA. That is, you will need to simulate the arrival of a train and the interactions with B's neighbouring signalboxes which enable its passage through the block sections.

# 5 Deliverables

Your submission should include the following:

- A statement of any assumptions you have made about the requirements;
- A diagrammatic presentation of your specification which includes all processes and their interconnections;
- A LOTOS specification of ABS based upon the specification given in figure 3. Note that you are being asked to build upon the given specification of a block section, *i.e.* you **must not** modify the definition of the `BS` process in anyway;
- A transcript of a session with LOLA which demonstrates that the basic `BLK_SEC` system is unsafe;
- A transcript of a session with LOLA which demonstrates the safe passage of a train through your model of ABS.

**This assignment should be submitted via the course work box located within the "crush area" by 12noon on Friday 13th December 2002. Note that this assignment can be attempted EITHER as a team of 2 OR as an individual. In the case of a team submission, equal marks will be awarded to both team members.**

# References


[1] S. Hall. *Modern Signalling Handbook* Ian Allan Publishing, 1996. ISBN 0-7110-2471-5

[2] L.P. Lewis. *Railway Signal Engineering (Mechanical)* Reissue of 1932 edition edited by J.H. Fraser (first published in 1912). ISBN 1-899890-04-1