Distributed Systems Programming (F29NM1)

Modelling & Formal Verification Assignment

Andrew Ireland

The Absolute Block System of Railway Signalling: An Exercise in Modelling & Formal Verification for a Distributed Concurrent System

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 Although largely superseded[1] by fully electronic systems, ABS represents an interesting case study in the modelling of a distributed concurrent system.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 model of ABS in Promela and verify your model with respect to a safety property using SPIN.

Background material on the operation of railways and ABS is presented in §2. The basis for a Promela model of ABS is presented in §3. In §4 the actual modelling and verification tasks you are to undertake are described. Finally, in §5 the basic structure of your assignment submission is detailed.

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

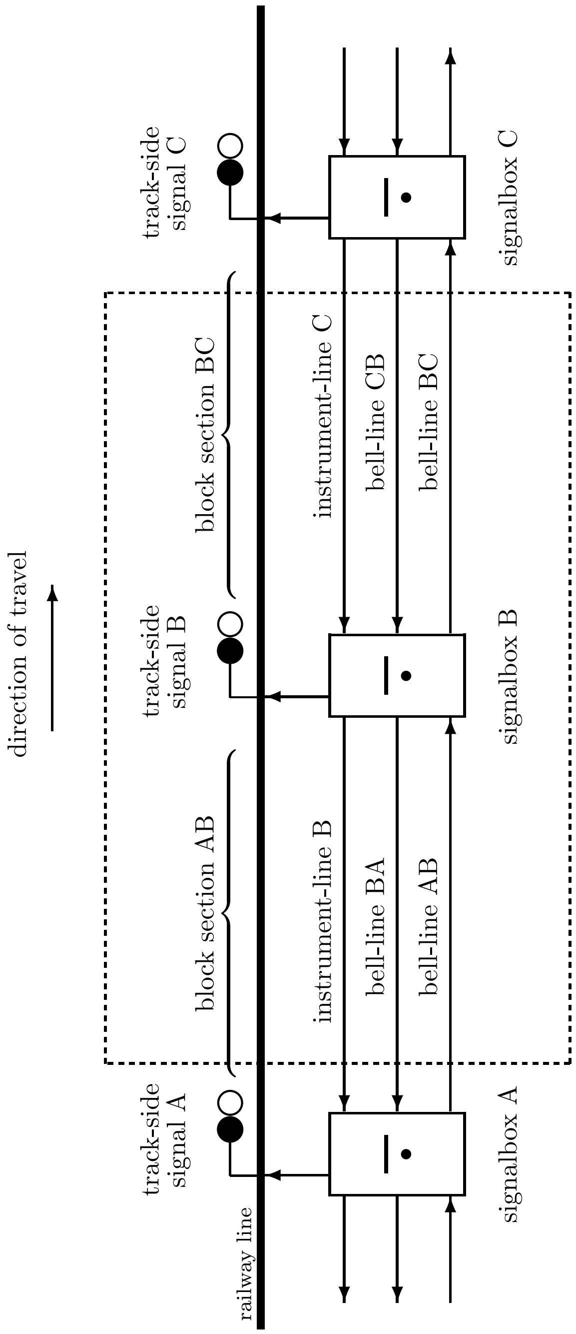
Within ABS railway lines are divided into a series of *block sections*. The aim of ABS is to ensure that only one train occupies the same line within a block section at the same time. ABS achieves this aim by positioning a *signalbox* between each block section. A signalbox has a human *operator*, the 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 topology of the ABS 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.

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 is 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.

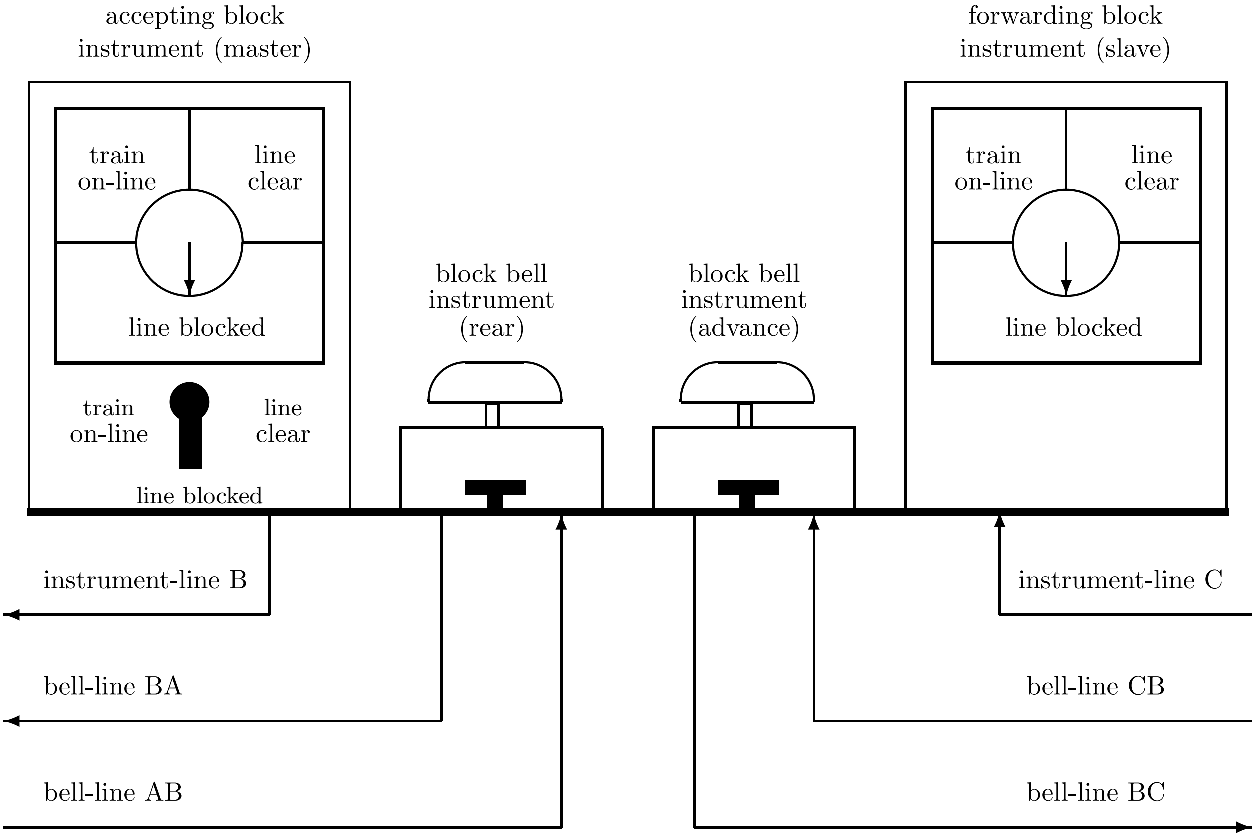
Meaning	**No. beats**	**Sequence**
call attention	1	1
is line clear for a train	4	3 pause 1
train entering section	2	2
train out of section	3	2 pause 1

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 neighbouring 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 An Unsafe Railway Network

A Promela model of an unsafe railway network is presented in Figure 3. The network involves 2 block sections of track, *i.e.* `BlockSecAB` and `BlockSecBC`. The block sections are modelled as channels, and the movement of trains is modelled by message passing, where a train is denoted by a 1 (bit). Signal processes are used to model the entry and exit of trains with respect to a block section. In the given network 3 signal processes are used, *i.e.* `SignalA`, `SignalB` and `SignalC`:

- `SignalA` allows an infinite sequence of trains to enter `BlockSecAB`;
- `SignalB` allows trains to exit `BlockSecAB` and then enter `BlockSecBC`;
- `SignalC` allows trains to exit `BlockSecBC`.

However these signal processes are **defective**, *i.e.* they do not regulate the safe passage of trains within the block sections. To be precise, they allow multiple trains to occupy the same block section of track at the same time. 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."*

In terms of the model presented in Figure3, this safety property can be represented within Promela by the following system invariant:

```
nfull(BlockSecAB) && nfull(BlockSecBC)
```

Note that `nfull` is true when applied to a non-full channel. Using SPIN's assertion verification capabilities, it is easy to show that the model violates the desired safety property.

4 Requirements

4.1 The Modelling Task

In terms of modelling, your task is to extend the Promela model given in Figure 3 so that it models the ABS as described in §2, *i.e.* so that it satisfies the safety property given in §3. Your extended model should meet the following requirements:

R1: The `SignalA`, `SignalB` and `SignalC` processes should be extended so that each of them models a physical track-side signal.

R2: 3 signalbox processes should be added, *i.e.* `SignalBoxA`, `SignalBoxB` and `SignalBoxC`. `SignalBoxB` should model the full ABS protocol as described in §2, *i.e.* the physical equipment within a signalbox as well as the actions which are performed by the signalbox operator. `SignalBoxA` and `SignalBoxC` should each model half of the ABS protocol, *i.e.* `SignalBoxA` should model only the forwarding mode while `SignalBoxC` should model only the accepting mode.

R3: `SignalBoxA` should control the track-side signal associated with `SignalA`, `SignalBoxB` should control the track-side signal associated with `SignalB` and `SignalBoxC` should control the track-side signal associated with `SignalC`.

```
#define train 1

chan BlockSecAB = [2] of { bit };
chan BlockSecBC = [2] of { bit };

proctype SignalA(chan out_track)
{
        do
        :: out_track!1
        od
}

proctype SignalB(chan in_track, out_track)
{
        do
        :: in_track?train;
           out_track!train
        od
}

proctype SignalC(chan in_track)
{
        do
        :: in_track?train;
        od
}

init {  atomic{
        run SignalA(BlockSecAB);
        run SignalB(BlockSecAB, BlockSecBC);
        run SignalC(BlockSecBC) }
}
```

A Promela model of an **unsafe** railway network is presented. The source for the model can be obtained via the following URL:

`http://www.macs.hw.ac.uk/ air/spin/handouts`

Figure 3: Model of an Unsafe Railway Network

Hints: A key feature of ABS is that a signalbox (operator) needs to know when a train has passed its track-side signal and has entered the block section in advance of its position, *e.g.* SignalBoxB needs to know when a train has left BlockSecAB and entered BlockSecBC. In the real world, this is achieved via track-circuits. In terms of the assignment, it is acceptable for the Signal process to perform this function, *e.g.* SignalB informs SignalBoxB when a train has left BlockSecAB and has entered BlockSecBC. Because there is **no** BlockSecCD, SignalC will need to inform SignalBoxC when the train simply leaves BlockSecBC.

Warning: the signalbox processes **should not** use `len`, `full`, `nfull` or `empty` in order to ensure the safe passage of a train. In addition, you should **not** use the `atomic` operator. **Note that your specification will be evaluated in terms of how accurately you have modelled the real-world instruments and procedures associated with the ABS signalling protocol.**

4.2 The Verification Task

You are also required to verify your system design with respect to the safety property given in §3. The safety property should be verified in two ways. Firstly it should be verified using SPIN's capability for reasoning about:

R4: system assertions.

Secondly, it should be verified using SPIN's capability for reasoning about:

R5: temporal properties.

In addition, you should:

R6: formulate and verify a response property with respect to your model.

5 Deliverables

Your submission should include the following:

D1: A statement of any assumptions you have made about the requirements.

D2: A diagrammatic presentation of your model which includes all processes and their interconnections.

D3: The Promela source for your extended railway network model.

D4: For each verification effort you should include the property that was verified together with a transcript of the associated "Verification Output" window.

This assignment counts for 50% of the course work mark for the module and should be submitted via the course work box located outside the student office (1.24) by **12noon on Friday December 7th, 2007. Note that this is an individual project which means that your submission MUST be your own work.**

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