Sender and Receiver System
Basic Properties

P1:

Sender can be in one of three states:

Inactive, Ready to Send, Finished Sending

Receiver can be in one of three states:

Inactive, Ready to Receive, Finished to Receive

P2:

Message channel contains at most n messages

P3:

Sender is inactive iff it sent a corresponding signal to the environment

Receiver is inactive iff it sent a corresponding signal to the environment

P4:

If Sender reached the Inactive state then it can not leave it until the Receiver has also reached its Inactive state

P5:

The decision of the Receiver whether to receive or whether to become inactive depends on the behavior of the Sender.
In this respect, no conflict arises.

P6:

The Receiver may only become inactive if the channel is empty and the Sender is Inactive.

Proving properties using Place Invariants

M(si) – denotes marking of place si, i.e. number of tokens located in this place

Property P1: It can be proven by using invariants i1 and i2:

$$M(s1) + M(s2) + M(s3) = 1 \qquad (i1)$$

$$M(s7) + M(s8) + M(s9) = 1 \qquad (i2)$$

Property P2: It indicates that channel is correctly controlled; this can be proven by invariant i3 that includes channel place s4, a complement of the channel place, and Receiver Inactive place s9:

$$M(s4) + M(s5) + n*M(s9) = n \qquad (i3)$$

Property P3: Sender can leave the Inactive state as a result of a signal from environment (place invariant i4). Receiver can leave the Inactive state as a result of signal from environment (place invariant i5):

$$M(s10) + M(s12) – M(s3) = 0 \qquad (i4)$$

$$M(s11) + M(13) – M(s9) = 0 \qquad (i5)$$

Places s10 and s12 represent environmental places for Sender.
Places s11 and s 13 represent environmental places for Receiver.

Property 4: If the Sender reached the Inactive state, then it cannot leave it until the Receiver has reached also its inactive state (place invariant i6).

$$M(s6) – M(s10) + M(s11) = 0 \qquad (i6)$$

S6 – place representing 'terminated message' channel
S10 – Sender's environment place
S11- Receiver's environment place

If $M(s6) = 1$ then $M(s10) = 1$

If $M(s6) = 0$ then $(M(s10) = 1$ and $M(s11) = 1)$

Property 5: Let t6 and t8 (transitions responsible for receiving Sender's termination message or being Inactive) be enabled by a marking reachable from the initial marking. As a result:

$$M(s4) >= 1 \text{ and } M(s5) >= n \text{ and } M(s8) >= 1$$

Let's take invariants i2 and i3 combined together (i.e. Receiver and control channel combined together). By adding three above inequalities we get:

$$M(s4) + M(s5) + M(s8) >= n+2$$

(this is an upper bound on the number of tokens in these three places).

$$M(s4) + M(s5) + M(s7) + M(s8) + (n+1)*M(s9) = n+1 \quad (i2+i3)$$

This implies that:

$$M(s4) + M(s5) + M(s8) <= n+1$$

Property P6: The receiver can reach the Inactive state only when t8 is enabled, i.e.

$$M(s5) >= n \text{ and } M(s6) >= 1 \text{ and } M(s8) >= 1$$

For such markings M, it has to be shown that:

1. $M(s4) = 0$ (i.e. channel is empty)

From invariant i3 we have:

$$M(s4) + M(s5) + n*M(s9) = n$$

Now, $M(s4) <= 0$, $M(s5) >= n$, $M(s9) >= 0$ (YES, the channel is empty – s4)

2. $M(s3) >= 1$ (i.e. Sender is Inactive)

Combining invariants i4 and i6 (Sender Inactive s3 + termination of messages – s6) together we get:

$[M(s6) + M(s12) + M(s11) – M(s3) = 0] \Rightarrow M(s3) >= M(s6) >= 1$