A Case Study: the RBC/RBC Handover Process

Ming Chai

Humboldt University of Berlin

Description of the RBC/RBC Handover Process

European Train Control System (ETCS) is a signaling, control and train protection system that is replacing the national, incompatible safety systems within Europe. ETCS consists of the on-board subsystem (composed of ERTMS/ETCS on-board equipment, the on-board part of the GSM-R radio system and specific transmission modules for existing national train control systems), and the track-side sub-system (composed of balise, lineside electronic unit, GSM-R, radio block center (RBC), euroloop and radio infill unit). In ETCS, the RBC is responsible for providing movement authorities to allow the safe movement of trains. A movement authority is generated by computing messages to be sent to the trains, where the messages are on the basis of information received from external track-side systems and information exchanged with the on-board subsystem. A route is divided into several RBC supervision areas. Here we consider the RBC/RBC handover specification. When a train approaches the border of an RBC supervision area, an RBC/RBC handover process takes place.

For an efficient handover, communication between two RBCs is required when a train is about to move from one RBC supervision area to the adjacent one (see Fig. 1).

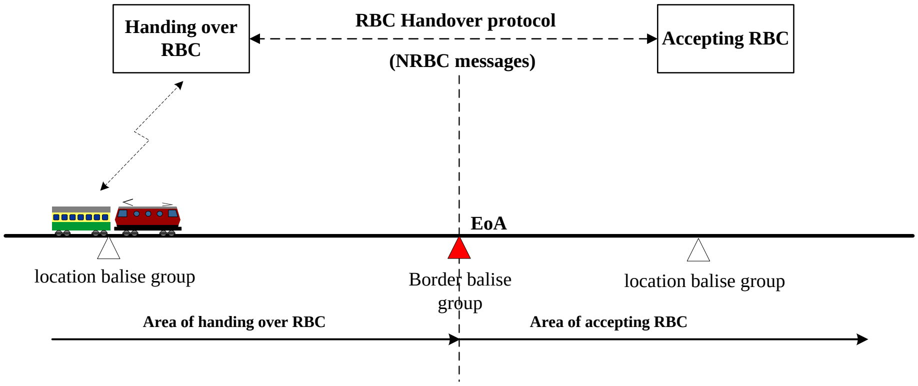

Fig. 1. RBC/RBC Handover

The NRBC messages are messages sent to or received from a neighbor RBC. The RBC/RBC handover transaction is defined as the sequence NRBC messages between RBCs to support the passing of a train from one RBC to an neighbor RBC. The RBC/RBC handover transaction is formally described with state diagrams (see Fig. 2) in the specification subset-039.

Events appearing in these handing over RBC state diagram and accepting RBC state diagram are specified in the appendix (Tab. 2 and Tab. 3).

Properties to be Monitored

The NRBC message are exchanged via GSM-R, which is an open communication system. An open communication system is "a transmission system with an unknown number of participants, having unknown, variable and non trusted properties, used for unknown telecommunication services and for which the risk of unauthorized access shall be assessed". The standard EN50159 identifies the following three categories of threats to an open transmission system:

- threats related to a message itself: corruption and masquerade;
- threats related to temporal relations of messages: repetition, deletion, insertion and resequencing;
- threats related to real-time request of messages: delay of a message.

A safety protocol is added between application layer and transport layer for providing safety communication between radio block centers (RBCs) (see. Fig. 3). The safety protocol ensures correctness of a message itself. It provides protection against threats related to corruption and masquerade. The temporal relations of messages are not covered by this protocol. The threats repetition, deletion, insertion and resequencing can be protected by monitors.

We specify the following properties with the eLSC language.exeuction

1. For a successful RBC/RBC handover process, if the HOV condition is detected, the NRBC messages PreAnn, RRI Req RRI and Ackn should be exchanged between the handing over RBC and the accepting RBC.

We specify this property with an eLSC specification as shown in Fig. 4. The messages preAnn and Ackn are exchanged in sequence if and only if the handing over RBC (HOVRBC) detects handover condition before. We specify the handover condition event by an "HOV cond" message . Therefore, the eLSC preHOV is with an "iff" prechart, which consists of the receiving event of the message HOV cond. If HOVRBC sends an RRIReq message to the accepting RBC (ACCRBC), and ACCRBC acknowledges the request, ACCRBC sends an RRI message to HOVRBC. HOVRBC sends an Ackn message to ACCRBC after receives the RRI message. Remark that the accepting RBC is allowed to send RRI without an RRI request when there is new route information. Hence, the eLSC ExdEoA is with a necessary prechart. Since the handing over RBC can ask for new route information iteratively, the eLSC ExdEoA is with an iteration.

According to the specification, the messages RRIReq and RRI is allowed to be exchanged after the handing over RBC and the accepting RBC are in the HOV

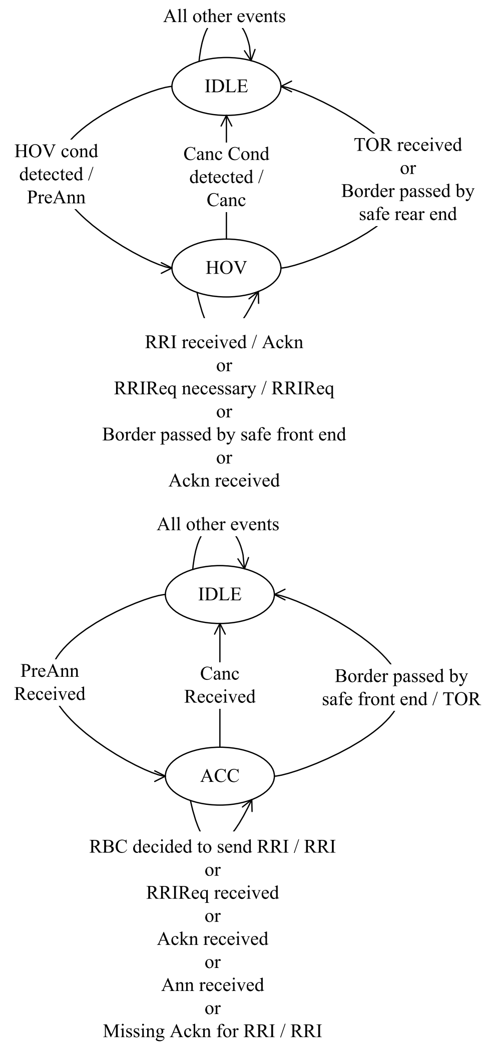
All other events
IDLE
HOV cond detected / PreAnn
Canc Cond detected / Canc
TOR received or Border passed by safe rear end
HOV
RRI received / Ackn or RRIReq necessary / RRIReq or Border passed by safe front end or Ackn received
All other events
IDLE
PreAnn Received
Canc Received
Border passed by safe front end / TOR
ACC
RBC decided to send RRI / RRI or RRIReq received or Ackn received or Ann received or Missing Ackn for RRI / RRI

Fig. 2. RBC/RBC handover transaction: the handing over RBC (left) and the accepting RBC (right)

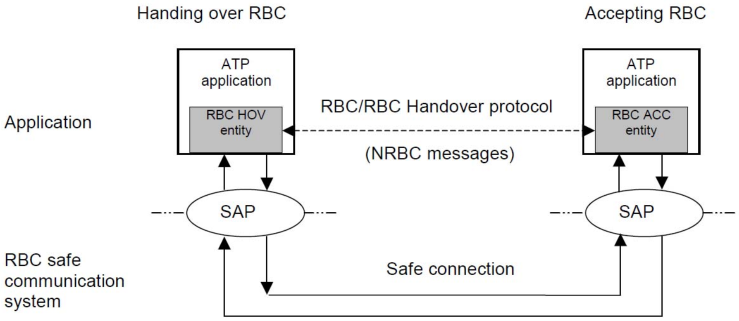

Fig. 3. Model of the RBC/RBC communication

and ACC states, respectively. The handing over RBC moves to the HOV state after sends a PreAnn message, and the accepting RBC moves to the ACC state after sends the acknowledgment message for PreAnn. Thus, the ExdEoA eLSC cannot be executed before the preHOV eLSC. To make the notations elegant, we introduce a strong concatenation (notated with a double line arrow) for the specification $\{(\mathfrak{m}_1, \mathfrak{m}_2, \mathit{Suff}), (\mathfrak{m}_1, \mathfrak{p}_2, \mathit{Suff})\}$.

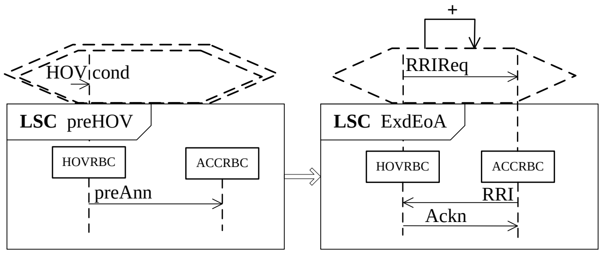

Fig. 4. eLSC Specification for Property 1

2. If and only if a cancellation condition is detected, the handing over RBC sends a cancellation message to the accepting RBC later. This property is specifies with an eLSC with an "iff" prechart (see Fig. 5).

3. The NRBC messages can not exchange without a safe connection between the two RBCs is established. The safe connection is set-up according to the specification subset-037. In the context of the RBC/RBC handover process, the handing over RBC is the calling safety service (SaS) user, whereas the accepting RBC is the called SaS user. The safe connection is established after the calling SaS user (i.e., the handing over RBC) receives a "safe connection confirm" (Sa-CONN.conf) message. Take the preAnn message as an example, the eLSC specification for this property is: the preAnn message cannot be exchanged be-

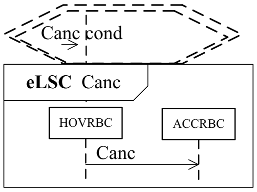

Fig. 5. eLSC for Property 2

fore HOVRBC receives a Sa-CONN.conf message. The eLSC is shown in Fig. 6. Other NRBC messages can be specified with the same manner.

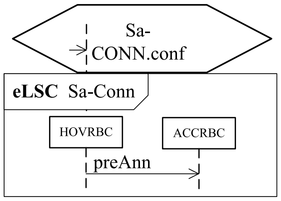

Fig. 6. eLSC for Property 3

4. The RBC/RBC handover succeed: if and only if the condition "Border passed by safe front end" is detected, the accepting RBC sends a “taking over responsibility” message to the handing over RBC later. The eLSC is shown in Fig. 7.

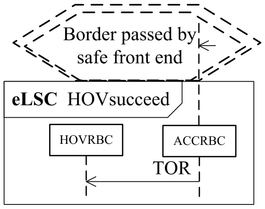

Fig. 7. eLSC for Property 4

Traces to be Monitored

We build two traces τ_1 and τ_2 according to the requirement of ETCS. In addition, we build traces τ_3, τ_4 and τ_5 with injecting some errors, such as adding/removing some events, and exchanging occurrence orders of some events. These traces are shown in Fig. 8 and Fig. 9.

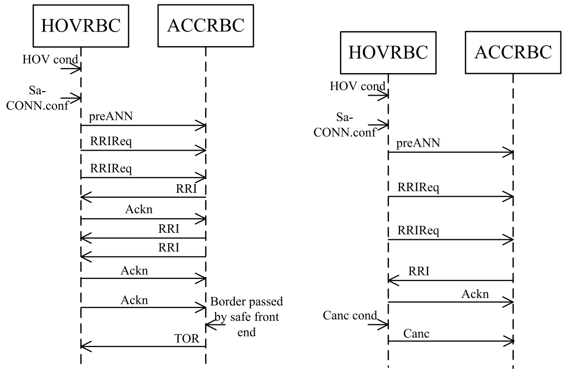

Fig. 8. Example traces: τ_1 (left) and τ_2 (right)

The monitoring results are presented in Table 1.

Table 1. Monitoring results

	Pro1	Pro2	Pro3	Pro4	Conclusion
τ_1	true	true	true	true	safe
τ_2	false	true	true	true	safe
τ_3	true	true	false	false	unsafe
τ_4	false	true	true	true	unsafe
τ_5	false	true	true	true	unsafe

The trace τ_1 satisfies all monitoring properties. It is a correct execution. The trace τ_2 violates the property 1. Therefore, it does not exhibit a successful RBC/RBC handover process. Since τ_2 satisfies the cancellation property (i.e., the property 2) and the cancellation condition is detected (by receiving the "Canc cond" message), the trace τ_2 is also a correct execution.

The trace τ_3 exhibits an execution, in which some messages are not transmitted via safety protocol; and the accepting RBC take over the train before the safe front end of the train passes border. The trace τ_4 exhibits an execution, in which the accepting RBC of eLSCdoes not send RRI after receives RRI request. The trace τ_5 exhibits that the handover RBC receives an RRI which is not send by the accepting RBC. Monitors can detect all these incorrect traces. In fact, some of these execution may lead to failure of the ETCS. For example, in the trace τ_5, the train runs under an incorrect (maybe an expired) move authority. If there is another train in front, train crash may happen.

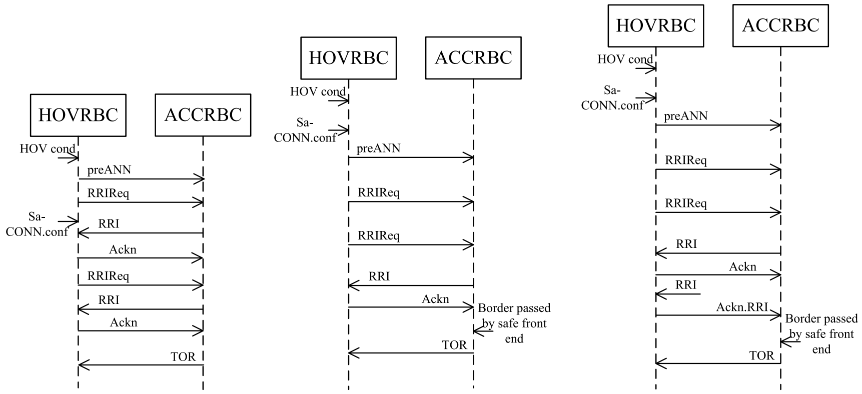

Fig. 9. Traces with errors: τ_3 (left), τ_4 (middle) and τ_5 (right)

We build traces by repeating the trace τ_1. The monitoring efficiency is shown in Fig. 10. Remark that the efficiency of property 2 is the same with property 4. The case study shows that eLSC based runtime verication implementation is feasible to detect failures in the executions of a system.

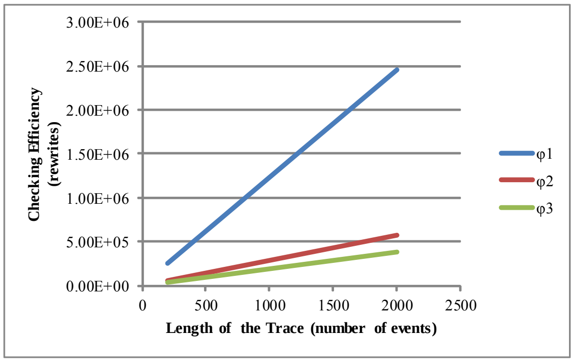

Fig. 10. Monitoring efficiency

Appendix

The incoming and out going messages of the hand ove RBC and the accepting RBC.

Table 2. Events of handing over RBC

Event	Type	Description
HOV cond	Incoming	Handover condition detected
RRIReq necessary	Incoming	Handing over RBC detects that route related information is required from the accepting RBC
RRI received	Incoming	NRBC message "Route Related Information" received
Border passed by safe front end	Incoming	Position report received and condition "Border passed by maximum safe front end" detected
TOR received	Incoming	NRBC message "Taking Over Responsibility" received
Border passed by safe rear end	Incoming	Position report received and condition "Border passed by minimum safe rear end" detected
Canc Cond detected	Incoming	Cancellation condition detected
Ackn received	Incoming	NRBC message "Acknowledgement" has been received
PreAnn	Outgoing	Send NRBC message "Pre-Announcement"
RRI request	Outgoing	Send NRBC message "Route Related Information Request"
Ackn	Outgoing	Send NRBC message "Acknowledgement"
Ann	Outgoing	Send NRBC message "Announcement"
Canc	Outgoing	Send NRBC message "Cancellation"

Table 3. Events of accepting RBC

Event	Type	Description
PreAnn received	Incoming	NRBC message "Pre-Announcement" received
RBC decided to send RRI	Incoming	Accepting RBC has decided (e.g. Signalling environment has changed) to send NRBC message "Route Related Information"
RRIReq received	Incoming	NRBC message "Route Related Information Request" received
Ackn received	Incoming	NRBC message "Acknowledgement" received
Ann received	Incoming	NRBC message "Announcement" received
Condition "Border passed by safe front end" detected	Incoming	Position report received and condition "Border passed by maximum safe front end" detected
Missing Ackn for RRI	Incoming	Acknowledgement for RRI not received, e.g. a timer expires
RRI	Outgoing	Send NRBC message "Route Related information"
TOR	Outgoing	Send NRBC message "Taking over Responsibility"
Ackn	Outgoing	Send NRBC message "Acknowledgement"