The description of moving block case study and modeling in SysML

Ehsan Poorhadi[1] and Elena Troubitsyna[1]

KTH – Royal Institute of Technology, Stockholm, Sweden
{poorhadi,elenatro}@kth.se

1 A Case Study: Moving Block

Our case study – a subsystem of the ERTMS/ETCS Level 3 moving block architecture [1]–is a typical example of NCS. The system aims at controlling trains' movement by using as few trackside devices as possible and relying on direct communication with trains. Radio-block centers (RBC) are deployed to deliver signals to trains and receive feedback. Each RBC controls the movement of the trains along a certain area by either authorizing them to move at a certain speed or stopping them. RBC sends to a train, passing through its area, a movement authority – a message containing among others danger point and end of the movement authority (EoA). A train is not allowed to pass its EoA to avoid hazardous situations. However, depending on the implementation, a safety margin might define a danger point to be beyond EoA. Therefore, the safety property usually is defined in terms of not passing the danger point, although, according to the definition, the train must not pass its EoA. In this case study, we aim to prove the safety property while the communication channel between the train and RBC is under attack.

We consider an attacker who performs a two-phase attack. First, she injects a valid movement authority message to set the value of EoA beyond the danger point defined by RBC. Such an attack constitutes a direct safety hazard since the EOA set by the attacker could be at the rear end of another train. Such an attack is shown to be possible in [2]. The authors exploit several vulnerabilities in communication protocols to forge a valid movement authority message. Therefore, the train accepts the forged message. In the second phase, the attacker actively monitors train-RBC communication and takes some actions e.g., dropping a message to prevent the detection of the attack and stopping the train before passing the intended EoA.

Our goal is to model and analyze the communication between RBC and the train to derive the conditions ensuring that the train would not pass the EoA, which is set by the attacker to be beyond the danger point determined by RBC. To do so, we define a control loop including RBC and train subsystems and apply our approach to determine necessary and sufficient conditions that guarantee safety in the presence of the attacker.

In the moving block case study, the controller is distributed between RBC and ATP – an Automatic Train Protection system installed in trains. ATP calculates the position of the train using measurements of *Odometer* and forms a

position report message to RBC. Then RBC estimates the train position and either does not send a message or sends an *Emergency stop* command, or sends other messages, which we treat as a heartbeat indicating that the communication is alive. Finally, ATP decides whether to send a brake command to the train braking system. In our study, the odometer corresponds to the sensor of the generic NCS architecture and the train's braking system to the actuator.

In the next section, we apply our modeling guidelines to represent the moving block case study in SysML. In addition, we discuss how we use HAZOP to identify different types of attack actions and model their impact on the component behavior.

References

1. ERTMS/ETCS signaling system, https://www.era.europa.eu/domains/infrastructure/european-rail-traffic-management-system-ertms_en.
2. Chothia, T.,Ordean,M., De Ruiter, J., Thomas, R.J.:An attack against message authentication in the ERTMS train to trackside communication protocols. In: Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, pp. 743–756. ACM (2017)