Implementing Rule-Based Anomaly Detection for Railway Signalling

TECHNISCHE UNIVERSITÄT DARMSTADT

Bachelor/Master Thesis

Train operation is controlled centrally from so called interlockings (de: Stellwerk). An operator sets train routes on the track and communicates clearances via Signals to the train driver. The interlocking and the field elements (signals, points, etc.) are connected via a communication network called railway signalling network. With the ubiquitous digitalization, commercial off-the-shelf protocols and products are introduced in the signalling networks. This requires a strong security concept that protects railway signalling networks from cyberattacks and thus the safety of people and cargo.

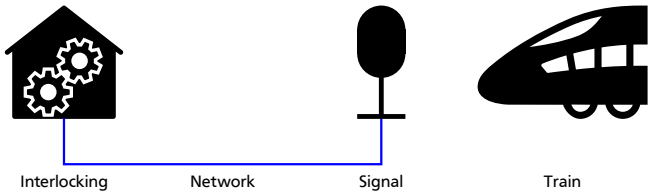

Figure 1: Architecture of a typical signalling network

Currently the field elements, driven by so called object controllers (OCs), blindly execute any command they receive from the interlocking. They are not able to distinguish the interlocking from an attacker impersonating it. One concept among many to enhance the security of the interlocking network is to make the signals smarter by enabling them to perform plausibility checks on the received commands and allow them the decision to obey it or not. By communicating with their neighbours, the field elements can determine whether it is safe to execute a command or if it leads to a harmful situation like derailment or collisions of trains. Our previous work has shown that such a concept indeed increases the security of railway operation.

Tasks

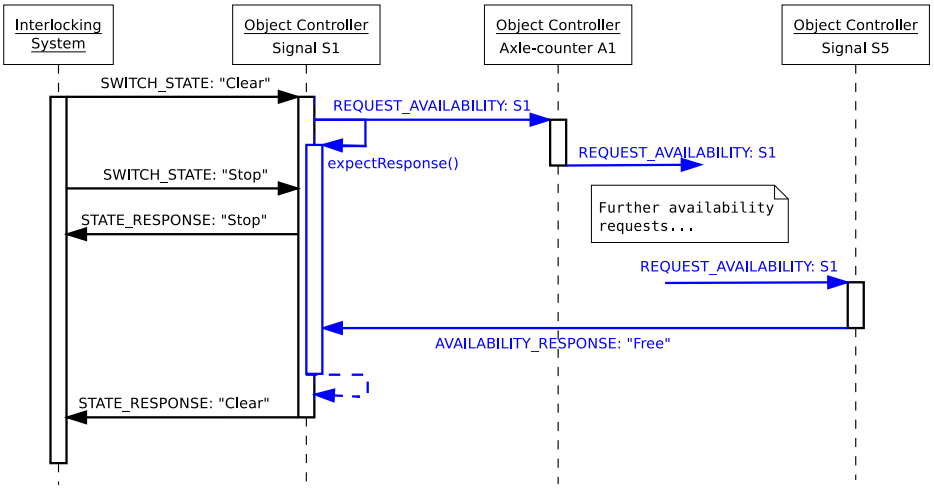

Figure 2: Communication scheme of a rule-based anomaly detection system

During this thesis, you will implement the rule-based anomaly detection system that we developed in previous work. The goal is to develop a working proof of concept (PoC) in our railway signalling lab and to document the necessary steps. Our lab provides you with the protocols (written in C) used in real-world interlocking networks, a model of railway infrastructure and an operating workstation that simulates the interlocking. After familiarizing with the utilized protocols, general communication in railway signalling and our rule-based anomaly detection concept, you will start with defining a strategy to establish the communication between the field elements that is demanded by our concept. You will implement the rule-based anomaly detection concept for our signalling lab. The concept has been evaluated in a centralized simulator before. Your PoC should show that it works also distributed on the many field elements comprising a signalling network. During the implementation in our signalling lab you will document the necessary design decisions as a part of your thesis.

Requirements

- Ability to work independently and be self-driven
- Knowledge in railway signalling is an asset
- Experience with programming languages: preferably C, C++, Java or Python
- Language: German or English (existing work is in English)

Markus Heinrich
Security Engineering Group
heinrich@seceng.informatik.tu-darmstadt.de
www.seceng.de

February 7, 2019