Chapter 2

The Model-Driven openETCS Paradigm for Secure, Safe and Certifiable Train Control Systems

Jan Peleska
University of Bremen, Germany

Johannes Feuser
University of Bremen, Germany

Anne E. Haxthausen
Technical University of Denmark, Denmark

ABSTRACT

A novel approach to managing development, verification, and validation artifacts for the European Train Control System as open, publicly available items is analyzed and discussed with respect to its implications on system safety, security, and certifiability. After introducing this so-called model-driven openETCS approach, a threat analysis is performed, identifying both safety and security hazards that may be common to all model-based development paradigms for safety-critical railway control systems, or specific to the openETCS approach. In the subsequent sections state-of-the-art methods suitable to counter these threats are reviewed, and novel promising research results are described. These research results comprise domain-specific modeling, model-based code generation in combination with automated object code verification and explicit utilization of virtual machines to ensure containment of security hazards.

INTRODUCTION

In 2009 German Railways initiated a discussion on a novel development paradigm for railway control systems. Motivated by concerns related to development costs, overall system quality, safety and security, they advocated the publication of re-usable control system code as Free/Libre Open Source Software FLOSS (Hase, 2009a; Hase, 2009b). The focus of this discussion was on the European Train Control System ETCS, because (1) as of today, ETCS is the most challenging European railway technology project, (2) the European Union has formulated explicit requirements...
regarding the introduction of ETCS in European countries, and (3) the public availability of the ETCS standard allows industries and research communities to perform analyses of and contribute to the ETCS concepts and technologies without infringing vendor-specific property rights. As one result of the initial discussions, a comprehensive list of development, verification and validation (V&V) artifacts was identified which should also be published under the FLOSS regime. These artifacts comprised specifications, designs and V&V results, such as correctness proofs, test suites and test results obtained with the publicly available software. Moreover, a well-defined open tool chain suitable for generating executable software code, V&V results and certification credits from these artifacts was advocated (Feuser & Peleska, 2010; Hase, 2011).

In this chapter the authors present a comprehensive workflow definition for developing railway control systems according to the FLOSS paradigm. We consider the following aspects of this exposition as our main contributions:

• It is described how the ETCS standard can be formalized using a modeling approach based on a domain-specific language (DSL). With this formalization at hand, concrete developments may be regarded as refinements and extensions of the abstract model represented by the standard, and conformance of the development to the standard can be established in a more rigorous way.
• The general openETCS paradigm is specialized to a model-driven openETCS paradigm, where developments focus on formally modeling the expected system behavior, while source code may be generated from the models in an automatic way.
• The workflow description is associated with a hazard analysis identifying the remaining safety and security threats still present when performing developments according to the model-driven openETCS paradigm.
• Effective methods for countering each hazard are described, so that the resulting development approach will guarantee a higher degree of safety and security and allow for more effective certification than the conventional approaches performed today by most of the railway suppliers.

The full ETCS standard covers train control computers, track elements and functionality to be integrated in track side interlocking systems. Following (Hase, 2011) we focus in this exposition on the train control computer, called the European Vital Computer EVC which is responsible for automated train protection (ATP). Observe, however, that the underlying paradigm, methodology and techniques described in this chapter are applicable to any railway control system development where

• A publicly available standard exists specifying system requirements in a generic way,
• A model-driven development and V&V approach is chosen, and,
• The contributing parties are willing to publish development and V&V artifacts according to the FLOSS principle.

BACKGROUND

In the original motivation of the openETCS initiative presented by Hase (2009a, 2009b, 2011), the author relates security issues observed in standard software products directly to threats to be expected in ETCS developments. For example, he argues that if backdoors could be integrated into standard commercial closed source products, the same could happen to railway control systems software. It should be emphasized, however, that
Related Content

How Much Automation can be Done in Testing?
[www.igi-global.com/chapter/much-automation-can-done-testing/62148?camid=4v1a](www.igi-global.com/chapter/much-automation-can-done-testing/62148?camid=4v1a)

Object-Role Modeling: Principles and Benefits
[www.igi-global.com/article/object-role-modeling/40952?camid=4v1a](www.igi-global.com/article/object-role-modeling/40952?camid=4v1a)

A Framework for Success in Real Projects for Real Clients Courses
[www.igi-global.com/chapter/framework-success-real-projects-real/29598?camid=4v1a](www.igi-global.com/chapter/framework-success-real-projects-real/29598?camid=4v1a)

Support Vector Machine: Itself an Intelligent Systems
[www.igi-global.com/chapter/support-vector-machine/21085?camid=4v1a](www.igi-global.com/chapter/support-vector-machine/21085?camid=4v1a)