UNIVERSITY OF BIRMINGHAM

School of Computer Science
College of Engineering and Physical Sciences

MSc. Project

A Formal Analysis of Train-Trackside Communications used in ERTMS

Submitted in conformity with the requirements
for the degree of MSc. Computer Security
School of Computer Science
University of Birmingham

Richard James Thomas, BSc. (Hons)
Student ID: 1156395
Supervisor: Dr. Tom Chothia

September 2015

MSc. Project
A Formal Analysis of Train-Trackside Communications used in ERTMS

Richard James Thomas BSc. (Hons)

Contents

Table of Abbreviations

- ATP – Automatic Train Protection
- CBC-MAC – Cipher Block Chaining Message Authentication Code
- CBTC – Communication Based Train Control
- DES – Data Encryption Standard
- ERTMS – European Rail Traffic Management System
- ETCS – European Train Control System
- GSM – Global System for Mobile Communications
- GSM-R – Global System for Mobile Communications for Railway
- IV – Initialisation Vector
- MAC – Message Authentication Code
- RBC - Radio Block Centre
- SaPDU – Safety Protocol Data Unit

TODO: Need to update this