



# 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

<b>1</b>	<b>Overview</b>	<b>1</b>
1.1	Abstract . . . . .	1
1.2	Acknowledgements . . . . .	1
<b>2</b>	<b>Introduction</b>	<b>2</b>
<b>3</b>	<b>The Current UK Rail Signalling Platform</b>	<b>3</b>
3.1	Overview . . . . .	3
3.2	Components . . . . .	3
3.2.1	Line-side Signals . . . . .	3
3.2.2	Occupancy Detection . . . . .	4
3.2.3	Communications . . . . .	4
3.2.4	Interlocking . . . . .	4
3.3	Issues . . . . .	4
3.3.1	Opportunity for Growth . . . . .	5
3.3.2	Infrastructure Failure . . . . .	5
3.3.3	Maintenance . . . . .	5
<b>4</b>	<b>The European Traffic Management System (ERTMS)</b>	<b>6</b>
4.1	Overview . . . . .	6
4.2	ERTMS Levels . . . . .	6
4.3	Protocols and Applications . . . . .	6
4.4	Components . . . . .	6
4.4.1	GSM-R . . . . .	7
4.4.2	Eurobalise . . . . .	7
4.4.3	Radio Block Centre (RBC) . . . . .	7
4.4.4	Driver Machine Interface . . . . .	7
4.4.5	ERTMS Systems Cab . . . . .	8
4.5	Case Study: Cambrian Line . . . . .	9
4.6	Vendor-specific Elements . . . . .	9
<b>5</b>	<b>GSM-R</b>	<b>10</b>
5.1	Overview . . . . .	10
5.2	Services Provided by GSM-R . . . . .	10
5.3	Infrastructure . . . . .	10
5.4	The use of GSM-R as part of ERTMS . . . . .	11
5.5	Weaknesses and Threats . . . . .	11
5.6	Looking to the Future of GSM-R . . . . .	12
<b>6</b>	<b>EuroRadio</b>	<b>13</b>
6.1	The EuroRadio Protocol . . . . .	13
6.2	EuroRadio Handshake Connection Protocol . . . . .	13
6.3	MAC Algorithm protecting Messages . . . . .	14
6.3.1	Importance of Proof of Knowledge . . . . .	15
6.3.2	Threats to EuroRadio as a Protocol . . . . .	15
6.4	Tools used in Formal Analysis . . . . .	16
6.5	Formally Modelling the EuroRadio Protocol . . . . .	16
6.5.1	Processes in Proverif . . . . .	17
6.6	Results . . . . .	17
6.6.1	Secrecy of Secret Value . . . . .	18
6.6.2	RBC Trust in the Train . . . . .	18
6.6.3	Train Trust in the RBC Generated Key . . . . .	18
6.6.4	RBC accepting data as a result of a train having sent it . . . . .	19
6.6.5	RBC accepting replayed messages . . . . .	19
6.7	High-Priority Messages . . . . .	21
6.7.1	Overview . . . . .	21
6.7.2	High Priority SaPDU Flow . . . . .	21

6.7.3	Permitted Messages and Format . . . . .	22
6.7.4	Threats . . . . .	22
6.7.5	Recommendations . . . . .	22
6.8	Threats to the MAC algorithm Cryptographically . . . . .	23
6.8.1	Recommendations . . . . .	24
6.8.2	Impact to implement security improvements . . . . .	25
6.9	Implementing Improvements to the EuroRadio Layer . . . . .	25
<b>7</b>	<b>Application Layer</b>	<b>26</b>
7.1	Overview . . . . .	26
7.2	Application Layer in detail . . . . .	26
7.2.1	Assumptions placed on the Application Layer . . . . .	26
7.2.2	Key Messages . . . . .	27
7.3	Safe Application Interface (SAI) Sublayer . . . . .	28
7.3.1	Defences offered by the SAI Sublayer . . . . .	28
<b>8</b>	<b>Other features of ERTMS investigated</b>	<b>30</b>
8.1	Key Management . . . . .	30
8.1.1	Overview . . . . .	30
8.1.2	Keys used in ERTMS . . . . .	30
8.1.3	Inserting keys on ERTMS Entities . . . . .	30
8.1.4	Key Derivation used in EuroRadio . . . . .	30
8.2	ERTMS versioning . . . . .	31
8.3	ERTMS as an Industrial Control System . . . . .	31
<b>9</b>	<b>Other Work</b>	<b>33</b>
<b>10</b>	<b>Project Evaluation</b>	<b>34</b>
10.1	Learning Opportunities . . . . .	34
10.2	Project Management . . . . .	35
10.2.1	Research Feedback . . . . .	36
10.3	Future Work . . . . .	36
10.3.1	RBC to RBC Communications . . . . .	36
10.3.2	Key Management . . . . .	36
10.3.3	CAN-BUS . . . . .	37
10.3.4	Eurobalises . . . . .	37
10.4	Legacy of the Project . . . . .	37
10.5	Critical Analysis and Personal Development . . . . .	38
<b>11</b>	<b>Conclusion and Summary</b>	<b>39</b>
	<b>References</b>	<b>40</b>
<b>12</b>	<b>Appendix One: Accompanying CD and Instructions</b>	<b>42</b>
12.1	Directory Structure . . . . .	42
12.2	How to Run the Platform . . . . .	42
<b>13</b>	<b>R Histograms for Analysis</b>	<b>43</b>

## 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