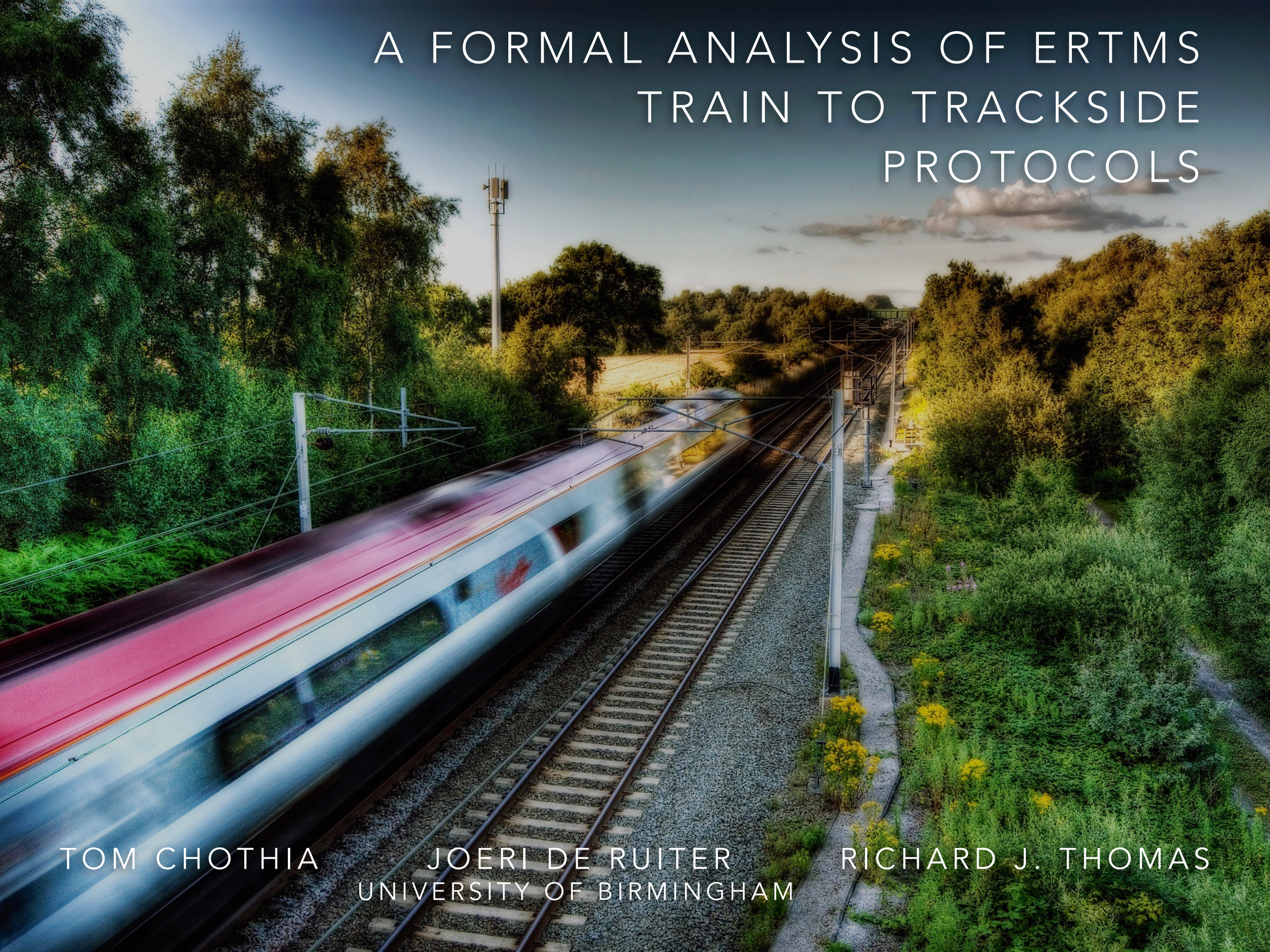
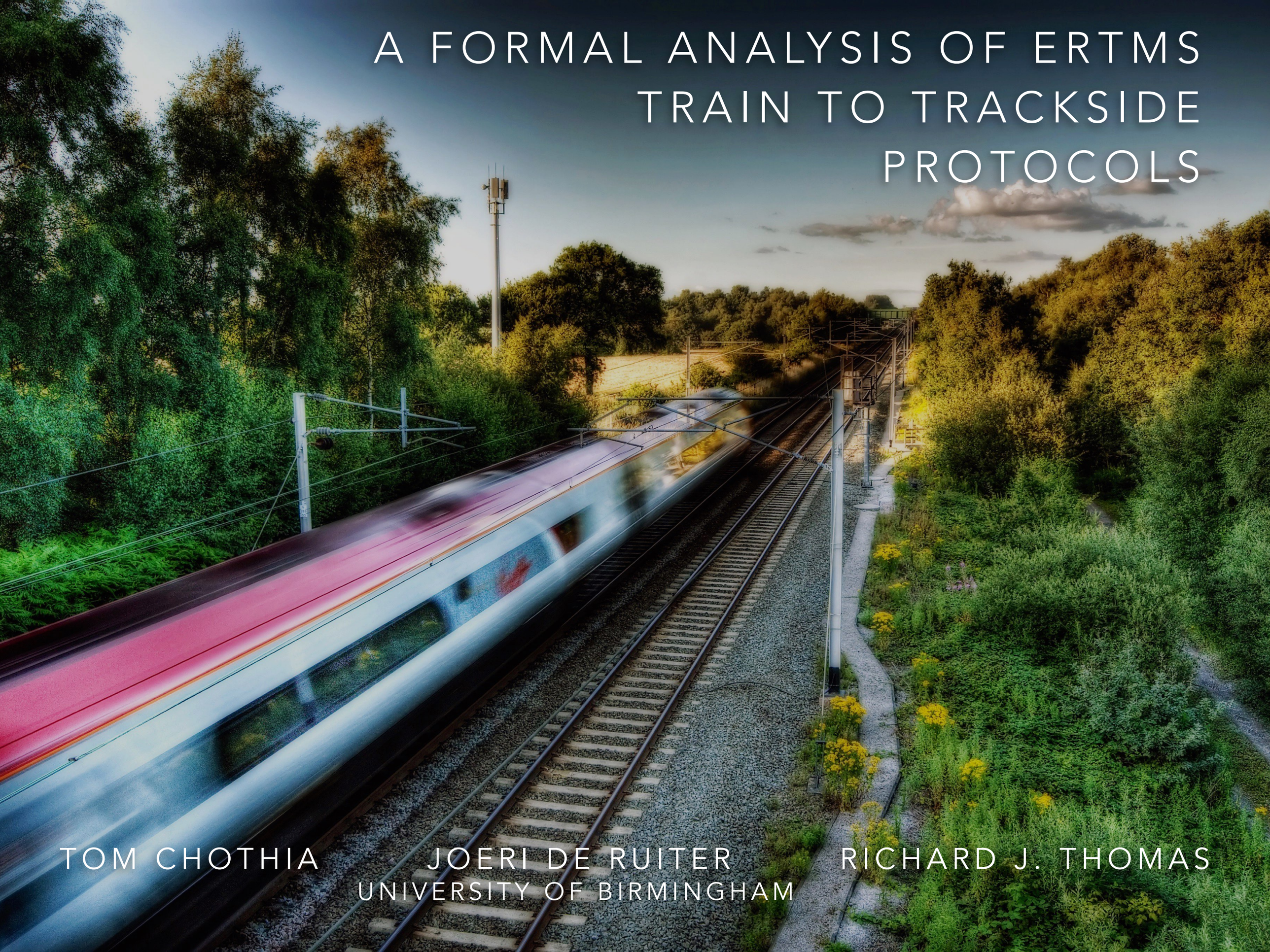


A FORMAL ANALYSIS OF ERTMS TRAIN TO TRACKSIDE PROTOCOLS

TOM CHOTHIA JOERI DE RUITER RICHARD J. THOMAS
UNIVERSITY OF BIRMINGHAM



A FORMAL ANALYSIS OF ERTMS TRAIN TO TRACKSIDE PROTOCOLS

TOM CHOTHIA JOERI DE RUITER RICHARD J. THOMAS
UNIVERSITY OF BIRMINGHAM

OUTLINE OF PRESENTATION

- Introduction
- What is ERTMS?
- ERTMS Communications Stack
- EuroRadio
  - Overview
  - Functions
  - Formal Analysis
- Application Layer
  - Modelling timestamps
  - Formal Analysis
- Recommendations
- Conclusion

INTRODUCTION

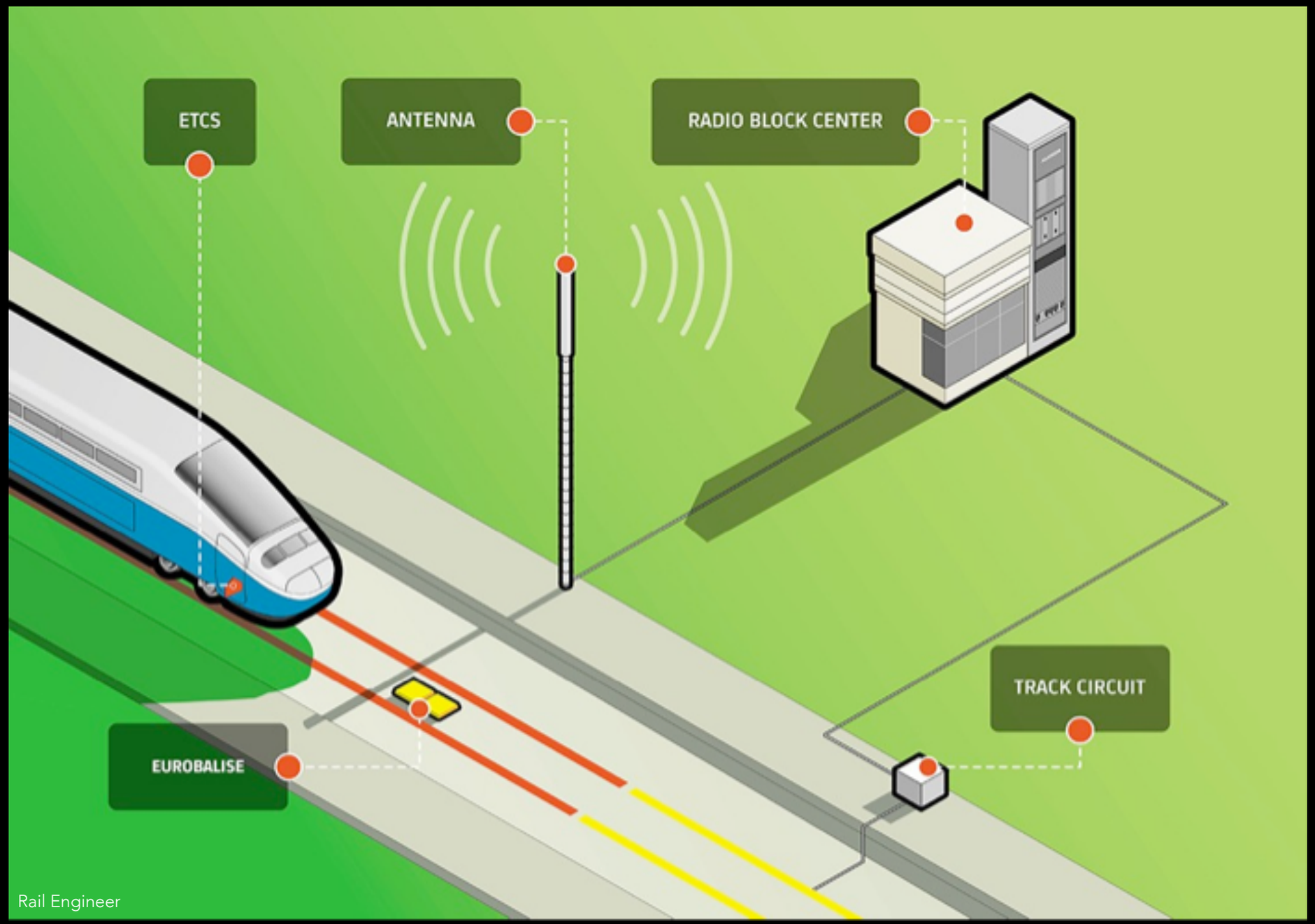
- ERTMS is an incoming European standard for **train management and signalling**
  - End of 2014 - half of the **80,000**km of track equipped with ERTMS located in Asia
  - **Wholly digitised**, supported by a number of protocols e.g. EuroRadio

- Moving from a largely analogue to a digital, fully supervised system **can expose the system to potential threats**

- Key to ensure that the infrastructure is **not susceptible to attack** which would compromise the safety-critical state of the railway

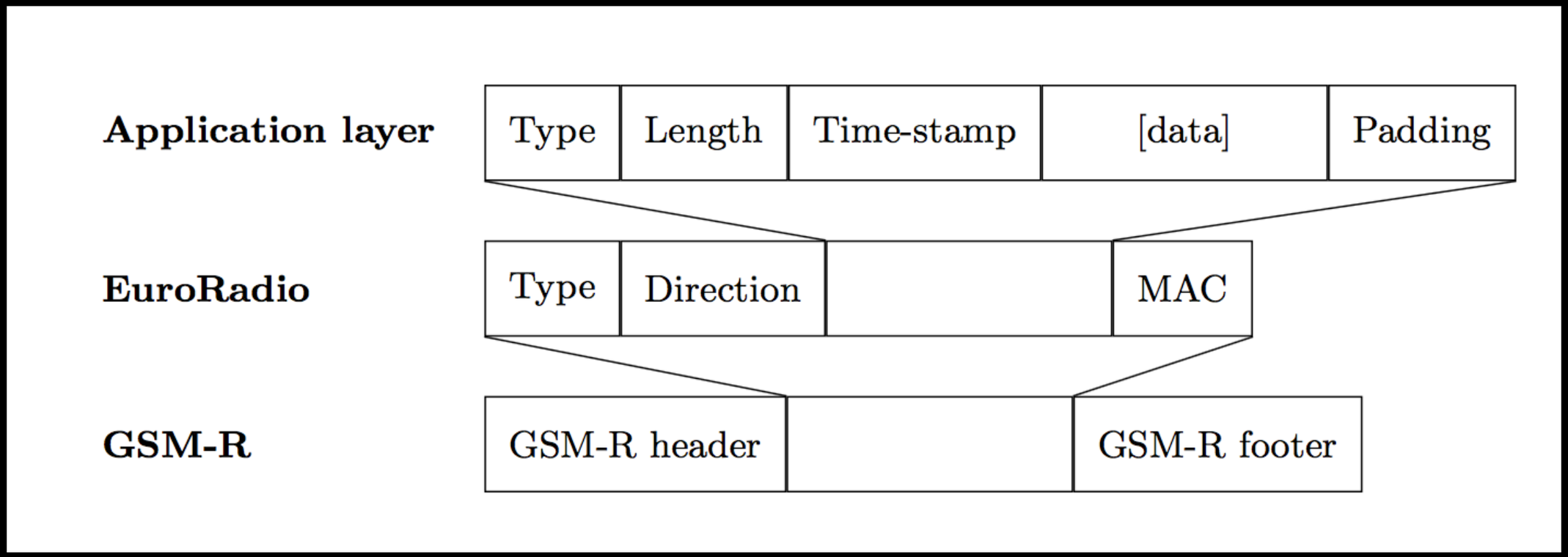
- **Formal analysis** allows protocols to be analysed from a security perspective
  - EuroRadio is mostly secure, but has some flaws

ERTMS COMPONENTS



Rail Engineer

ERTMS TRAIN TO TRACKSIDE COMMUNICATIONS STACK



GSM-R AND APPLICATION LAYER

- GSM-R
  - Extension of the GSM Standard for Rail applications
  - Currently used for communications between train and signallers in the UK
  - ERTMS will use this as the ‘umbilical cord’ for train-trackside communications
  - Offers additional facilities to GSM
    - Group Calling
    - Location Based Addressing
    - Emergency Calling

- Application Layer
  - Implements protection against **replay and deletion** attacks
    - Achieved through a 32-bit timestamp
    - Every message needs to have a timestamp greater than the previous message
      - Acts partly as a counter
    - RBC **maintains multiple clocks**, using the reference time from the train to synchronise the counters
  - Responsible for processing messages sent between train and trackside to the appropriate system

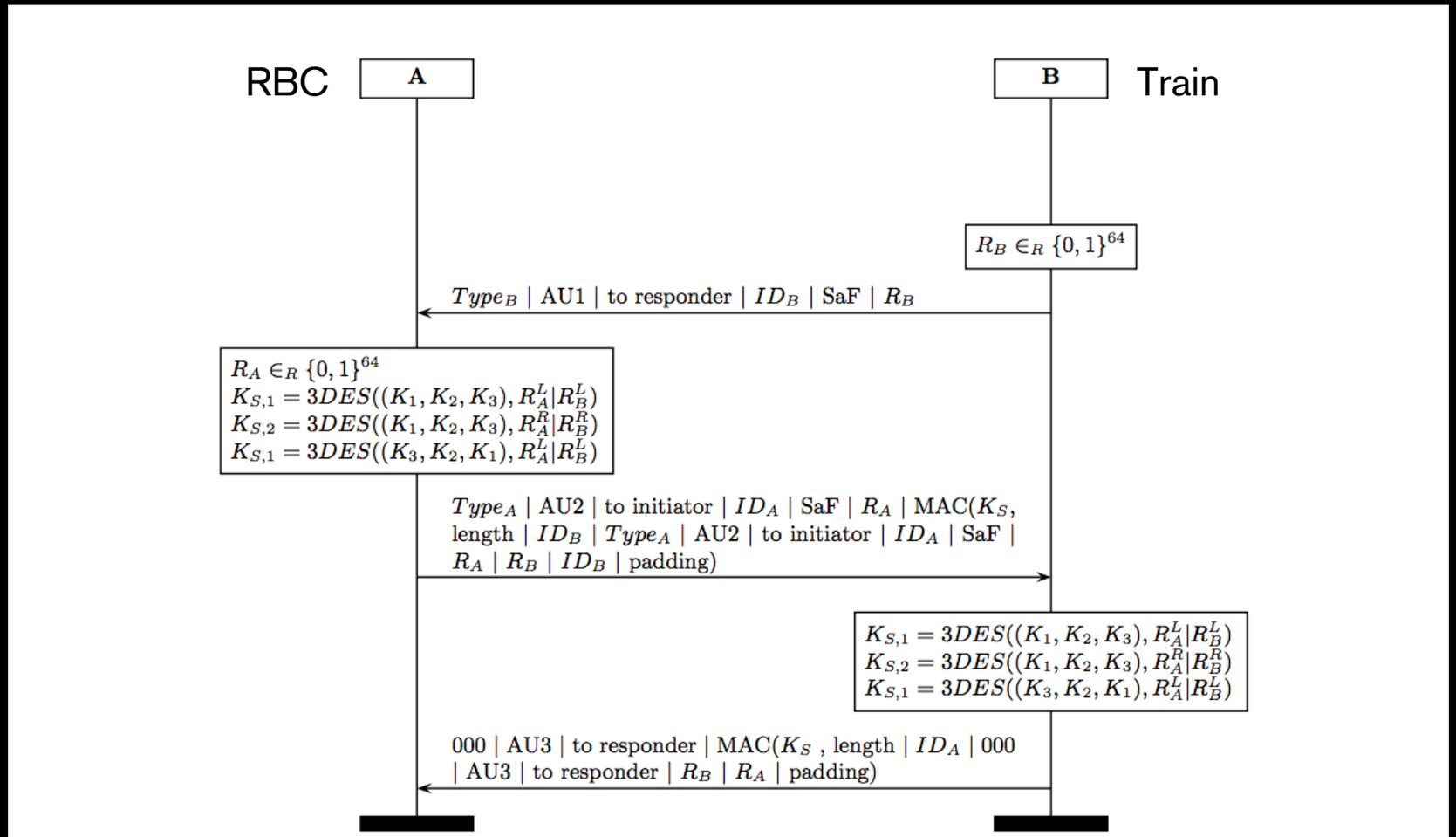
EURORADIO

FUNCTIONS, MESSAGE AUTHENTICATION,
CRYPTOGRAPHY, FORMAL ANALYSIS

EURORADIO OVERVIEW

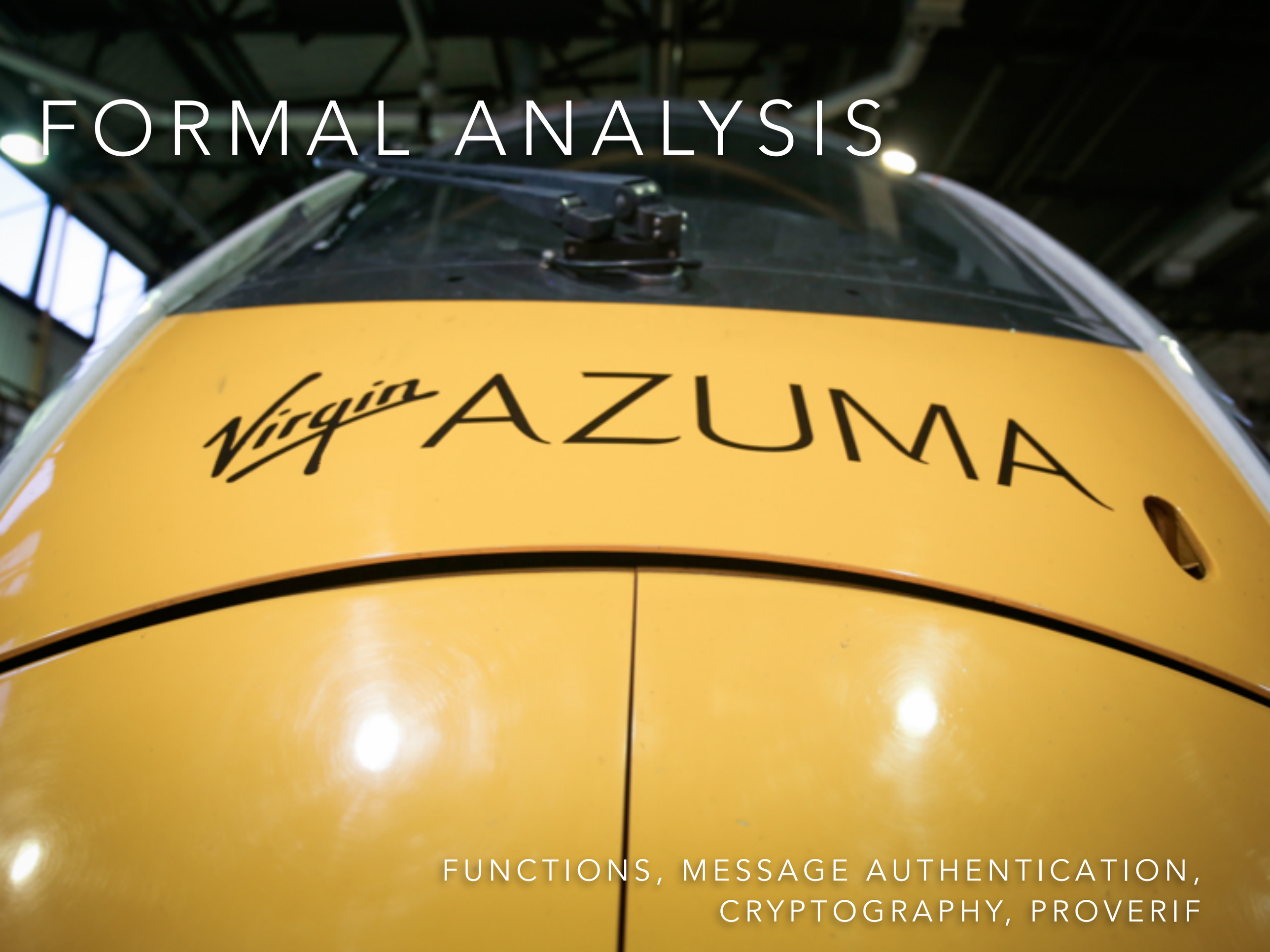
- Provides **authenticity and integrity** measures for any traffic sent between train and trackside
- **Authentication protocol** initiated once the GSM-R connection is established negotiates session keys mutually
- Session keys are **used to generate MAC** codes which are used to protect the message from being tampered ‘inflight’
  - Based on a shared train key and nonces exchanged as part of the authentication
- **All messages** sent as standard-priority messages will be accompanied by a MAC
  - The MAC used is negotiated through a **safety feature** negotiated during authentication.

EURORADIO PROTOCOL



Key	Description
AU_x	Authentication Message x
ID_x	ETCS Entity ID of party x
R_x	Nonce generated by party x
SaF	Safety Feature selected
To Initiator/Responder	Flag to indicate in which direction the message is being sent
$Type_x$	ETCS Entity ID type (e.g. RBC or train)

FORMAL ANALYSIS



FUNCTIONS, MESSAGE AUTHENTICATION,
CRYPTOGRAPHY, PROVERIF

FORMAL ANALYSIS

- Analysis performed using the **Proverif automated verifier**
  - Model performed verification of the authentication and ‘in-service’ elements of the protocol
  - MACs and timestamps added and verified
  - Model extended to consider high-priority messages

- Verified a number of properties for the layers (including **EN50159**)
  - Secrecy of Keys in EuroRadio
  - Mutual Authentication - Agreement on All Shared Values during Authentication
  - Ability to Insert Valid EuroRadio/Application Messages
  - Ability to Replay EuroRadio Messages
  - Ability to Reorder EuroRadio Messages
  - Ability to Block EuroRadio Messages without Receiver Knowing
  - Analysis of Emergency Messages in ERTMS

- Models available at https://www.cs.bham.ac.uk/~rjt195/rssrail2016

PROVERIF

- Automated protocol verifier using the **applied-pi calculus**
  - Can be used to identify potential information leakage or flaws in protocols
  - Allows declarations of processes which perform input/output operations which may **self-replicate** or **run in parallel**
  - **Functions** allow us to **abstract cryptographic primitives** e.g. MACs, signing and key generation
    - Focus is on analysing the protocol, **not** cryptographic implementations
    - Provides **guarantees for soundness**, but it is **not complete**

- Mainly security-focussed
  - Identifying traceability attacks in ePassports (Chothia et al 2010)
  - Identifying flaws in the Visa PayWave Contactless Protocol (Chothia et al 2015)

- Alternative formal analysis tools available
  - CryptoVerif
  - Tamarin Prover

MODELLING EURORADIO

- Train and RBC individually modelled to test properties against these processes
- Lightweight model of time defined to verify whether reordering possible

```
(* Support for relative time *)
data inc/1.
pred greater/2.
clauses
  greater: inc(x),x;
      greater: x,y -> greater: inc(x),y.
```

- ProVerif allows the model to capture an arbitrary number of attackers, processes and runs.
  - An attacker may then use values it learnt from previous sessions to attempt an attack in a different session.

SECURITY PROPERTIES

- A number of properties assessed:
  - Secrecy of Keys in EuroRadio
  - Mutual Authentication - Agreement on All Shared Values during Authentication
    - e.g. MAC Algorithm and identities of the conferring parties
  - Ability to Insert Valid EuroRadio/Application Messages
  - Ability to Replay EuroRadio Messages
  - Ability to Reorder EuroRadio Messages
  - Ability to Block EuroRadio Messages without Receiver Knowing
  - Analysis of Emergency Messages in ERTMS

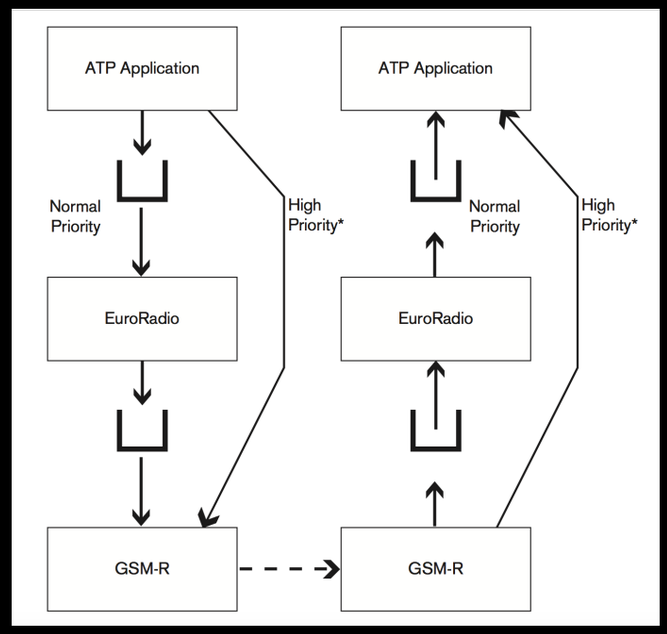
- Modelling of timestamps
  - Light-weight notion of counter-style timestamps defined and tested

FORMAL ANALYSIS USING PROVERIF

DEMO

FINDINGS

- Attacker **cannot learn the cryptographic keys**, nor can they establish plaintext of messages encrypted with the session key.
- Train and RBC are able to **agree on a shared session key**
- It is **possible for the attacker to 'redirect' messages** from the train to another RBC and potentially use a different Safety Feature
- Attacker **cannot insert their own messages** (given they do not have the session key to generate valid MACs)
- The attacker **cannot replay messages**, given that the timestamps on the application layer would detect this
- The **reordering of messages is not possible** but it is possible to prevent messages from being received, where timeouts and acknowledgements are the only way for this to be detected
- The **lack of MACs on high-priority messages** allow the attacker to send emergency stops



THREATS AND SOLUTIONS

DISCUSSION

- **High-priority messages may be inserted and accepted**
  - No protection is offered in the current standard
  - A train could therefore be convinced to stop arbitrarily

- **Messages may be deleted**
  - A train may need to be instructed to reduce its movement authority
  - Not being able to know if a message was deleted could lead to an unsafe state

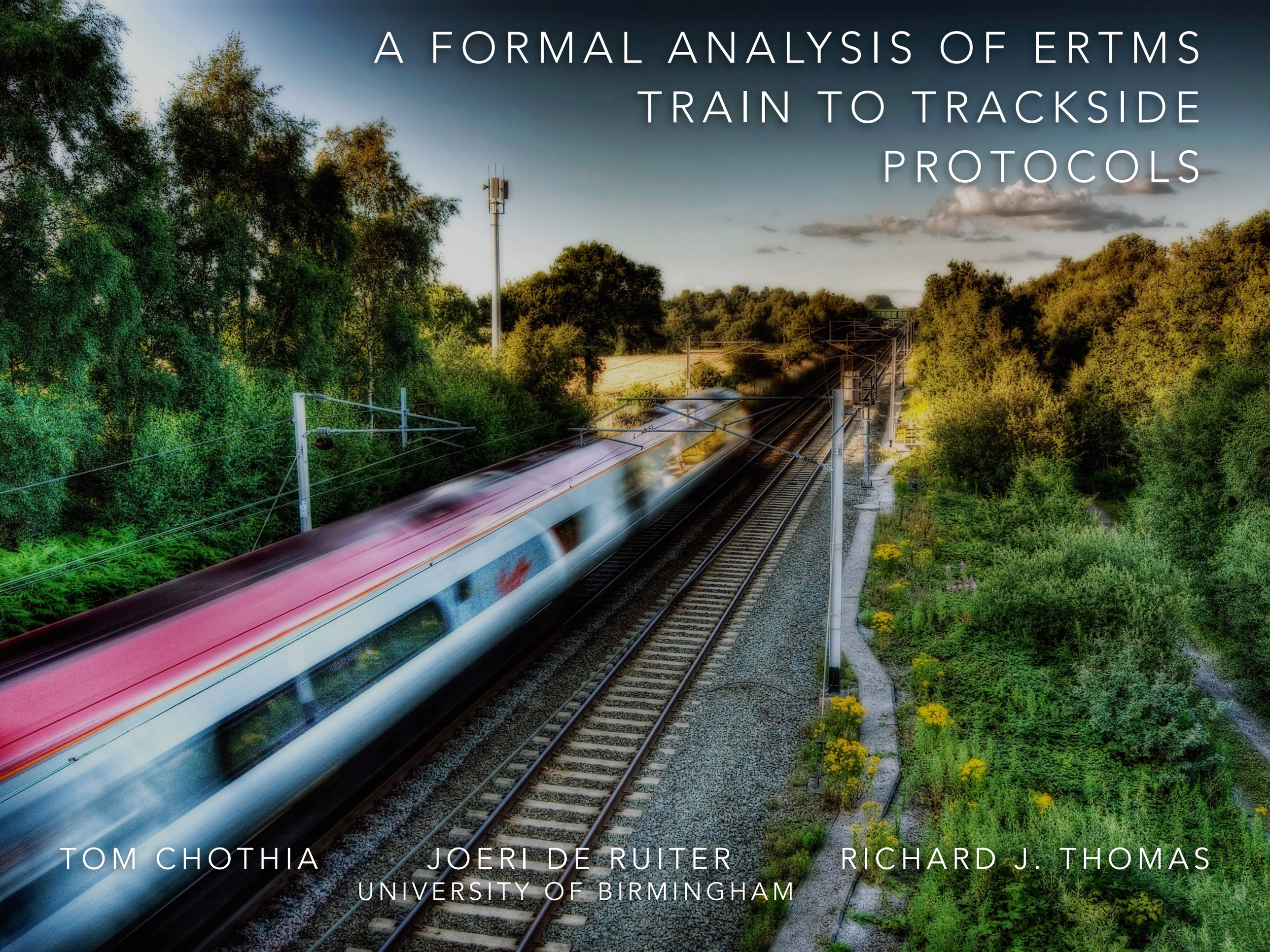
- **Attacker convincing the train to use a different RBC**
  - A train at Birmingham New Street may be rerouted to Edinburgh
    - Edinburgh RBC may ask the train to pull forward to obtain its location from the next balise
    - Moving the train forward could have serious consequences

- **Safety feature not explicitly checked**
  - Current standard specifies one MAC algorithm
    - New ones may be introduced. We should use either the one we specify ourselves as initiator or at least something more secure if proposed by the RBC.

RECOMMENDATIONS

- **Inserting unauthenticated high-priority messages**
  - Solution: add MAC to the high-priority message, but maintain priority over other messages.
- **Deletion of messages**
  - Solution: add counter to all messages, to track missing messages.
  - Use of the *M_NVCONTACT* and *T_NVCONTACT* parameters could be better to ensure that the safety-critical state is maintained.
- **Disagreement over RBC Identity and Safety Feature**
  - Solution: RBC ID should be verified during authenticiation and provision in the specifications made if the one specified locally does not match that recieved. If the Identity does not match, the connection should be dropped and EuroRadio authentication restarted.
  - Solution: The selected Safety Feature received by the sender should either be equal or more secure than what was sent to the initiator.

CONCLUSION



A FORMAL ANALYSIS OF ERTMS TRAIN TO TRACKSIDE PROTOCOLS

TOM CHOTHIA JOERI DE RUITER RICHARD J. THOMAS
UNIVERSITY OF BIRMINGHAM