



UNIVERSITY OF  
BIRMINGHAM



BCRRE

RITICS



CENTRE FOR  
CYBER SECURITY  
AND PRIVACY

UKRRIN  
UK RAIL RESEARCH AND  
INNOVATION NETWORK

# Cyber Security in the Rail Sector – An Integrated Approach

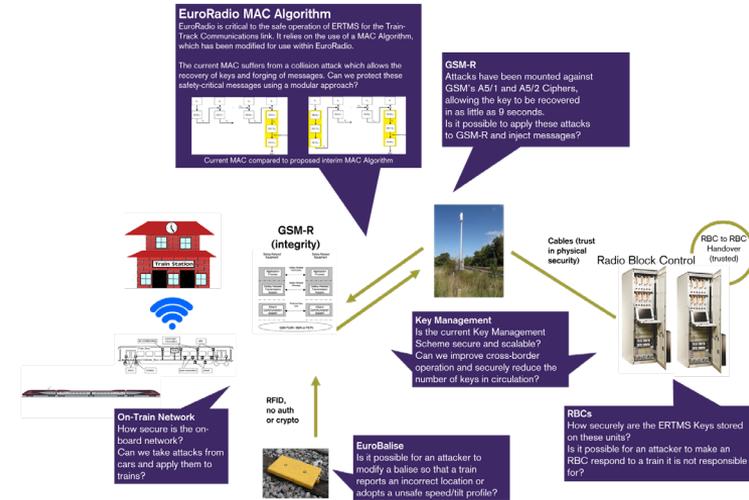
Richard J. THOMAS (R.J.Thomas@bham.ac.uk), Mihai ORDEAN, Tom CHOTHIA

University of Birmingham | [railway.bham.ac.uk](http://railway.bham.ac.uk)



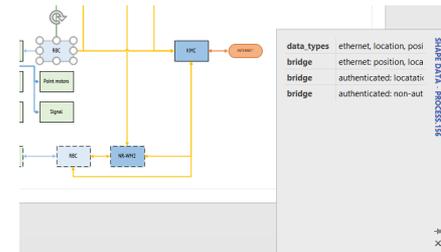
# The Challenge

- Focus on safety and functionality over security
- Cyber security incidents (e.g., INCONTROLLER) leveraging the inter-connected nature of systems to attack systems
- Meeting the requirements of the NIS Directive, TS 50701 and ISO/IEC 62443 presents a **significant knowledge and skills gap in rail cyber security**
- *How do we evaluate the threats and risks to our systems to drive improvements in rail cyber security?*



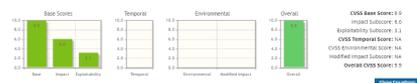
# The SCEPTICS Modelling Tool

- Visio-based tool allowing **rail engineering teams to diagram system architectures at any scale** (granular or generic)
- **Bridges** cyber security expertise with rail asset domain knowledge
- Applies the **CVSS Framework** to define the properties of the asset and what the impact is if compromised (e.g., loss of availability or impact on peer systems).
- Establishes **the risk of compromise and exploitation across complex systems-of-systems** in a probabilistic way and enables experimentation to get a ground-truth
- Types of Analysis
  - ‘All Roads Lead to’, ‘Patient Zero’ and testing of new strategies



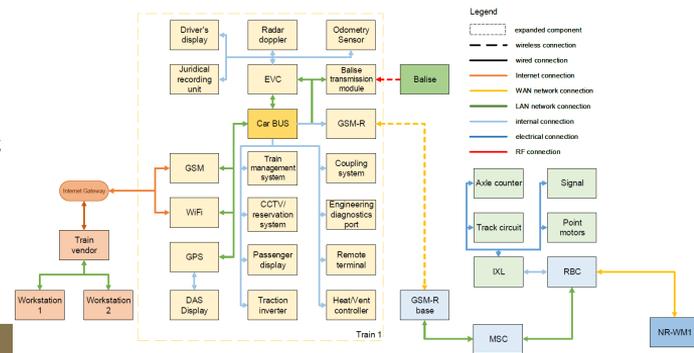
## Common Vulnerability Scoring System Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS Base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.



### Base Score Metrics

Metric	Value	Impact
Attack Vector (AV)	Network	High
Attack Complexity (AC)	Simple	Low
Privileges Required (PR)	None	Low
User Interaction (UI)	None	Low
Scope (S)	Unchanged	Low
Confidentiality Impact (CI)	None	Low
Integrity Impact (II)	None	Low
Availability Impact (A)	None	Low



# Applying the SCEPTICS Tool to ERTMS

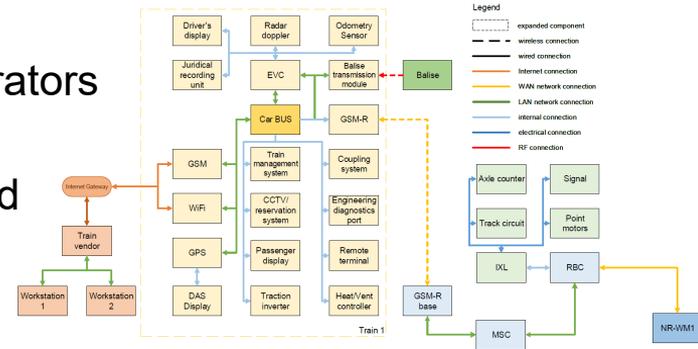
- Complex, interdependent architecture with multiple organisations, asset managers and maintenance operators
- Modelled ERTMS and on-board train systems in the SCEPTICS tool, and validated the security profiles and outputs with asset owners and stakeholders
- Ran the tool to see:

If a compromised balise would affect the EVC and result in an errant Movement Authority

Whether a compromised 3<sup>rd</sup> party could affect on-board systems

What the effect of GPS spoofing is

How investments (e.g., secure balises) reduce the risk to the railway



```
Adversary a1:
[Balise]->[Balise transmission module]->[EVC]:0.32736
[Balise]->[Balise transmission module]->[EVC]->[GSM-R]->[GSM-R base]->[MSC]->[RBC]:0.00016
[Balise]->[Balise transmission module]->[EVC]->[GSM-R]->[GSM-R base]->[MSC]->[RBC]->[RBC]->[RBC]:0.00016
->[GSM-R base]->[GSM-R]->[EVC]:0.32747
[SecureBalise]->[Balise transmission module]->[EVC]:0.06591
[SecureBalise]->[Balise transmission module]->[EVC]->[GSM-R]->[GSM-R base]->[MSC]->[RBC]:0.00006
[SecureBalise]->[Balise transmission module]->[EVC]->[GSM-R]->[GSM-R base]->[MSC]->[RBC]->[RBC]:0.00006
->[RBC]->[RBC]->[GSM-R base]->[GSM-R]->[EVC]:0.06597
```

```
Adversary a2:
[Workstation1]->[Train vendor]->[Internet Gateway]->[WiFi]->[Car BUS]:0.13456
[Workstation1]->[Train vendor]->[Internet Gateway]->[WiFi]->[Car BUS]->[Car BUS]:0.03276
[Workstation2]->[Train vendor]->[Internet Gateway]->[WiFi]->[Car BUS]:0.0313
[Workstation2]->[Train vendor]->[Internet Gateway]->[WiFi]->[Car BUS]:0.00762
```

```
Adversary a3:
[GPS]->[DAS Display]:0.97222
[GPS]->[Car BUS]->[Passenger display]:0.9452
[GPS]->[Car BUS]->[EVC]->[GSM-R]->[GSM-R base]->[MSC]->[RBC]:0.00085
```



# Conclusion

- The pace of digitalisation in the rail sector means cyber security is a critical issue, where threat and risk assessments help to manage the risk
- Rail Cyber Security has a significant skills and competency gap, where the SCEPTICS Tool empowers railway engineers to understand cyber security risks to their infrastructures without being experts
- Knowing what's vulnerable and a risk is one aspect, where the SCEPTICS tool supports decision-making for investments to protect assets today, tomorrow and into the future
- Full paper and tool available from **[research.rjthomas.io/wcrr2022-sceptics](https://research.rjthomas.io/wcrr2022-sceptics)**

