# Threat Catalogue

## Disclaimer

This document is drafted by and belongs to EU Rail.

EU Rail encourages the distribution and re-use of this document, the technical specifications and the information it contains. EU Rail holds several intellectual property rights, such as copyright and trade mark rights, which need to be considered when this document is used.

EU Rail authorizes you to re-publish, re-use, copy and store this document without changing it, provided that you indicate its source and include the following mention [EU Rail trade mark, title of the document, year of publication, version of document, URL].

EU Rail makes no representation or warranty as to the accuracy or completeness of the information contained within these documents. EU Rail shall have no liability to any party as a result of the use of the information contained herein. EU Rail will have no liability whatsoever for any indirect or consequential loss or damage, and any such liability is expressly excluded.

You may study, research, implement, adapt, improve and otherwise use the information, the content and the models inthis document for your own purposes.  If you decide to publish or disclose any adapted, modified or improved version of this document, any amended implementation or derivative work, then you must indicate that you have modified this document, with a reference to the document name and the terms of use of this document. You may not use EU Rail’s trademarks or name in any way that may state or suggest, directly or indirectly, that EU Rail is the author of your adaptations.

EU Rail cannot be held responsible for your product, even if you have used this document and its content. It is your responsibility to verify the quality, completeness and the accuracy of the information you use, for your own purposes.

## Maintenance

After release, this document immediately enters the maintenance phase. Maintenance includes error corrections and general improvement of the document. Please send your change requests to the following email address: cybersecurity.review@ertms.be

# ERORAT v3 Threat Catalogue

Note: this threat catalog is used in this version of the specification. The catalog is based on BSI publications. ERORAT v3 and the corresponding Security Guideline are available on https://ertms.be/activities/ertms-security-core-group.

| |
|---|
| G 0.13 Interception of Compromising Interference Signals |
| G 0.14 Interception of Information / Espionage |
| G 0.15 Eavesdropping |
| G 0.16 Theft of Devices, Storage Media and Documents |
| G 0.17 Loss of Devices, Storage Media and Documents |
| G 0.19 Disclosure of Sensitive Information |
| G 0.20 Information or Products from an Unreliable Source |
| G 0.21 Manipulation of Hardware or Software |
| G 0.22 Manipulation of Information |
| G 0.23 Unauthorised Access to IT Systems |
| G 0.24 Destruction of Devices or Storage Media |
| G 0.28 Software Vulnerabilities or Errors |
| G 0.29 Violation of Laws or Regulations |
| G 0.30 Unauthorised Use or Administration of Devices and Systems |
| G 0.31 Incorrect Use or Administration of Devices and Systems |
| G 0.32 Misuse of Authorisation |
| G 0.35 Coercion, Blackmail or Corruption |
| G 0.36 Identity Theft |
| G 0.37 Repudiation of Actions |
| G 0.38 Misuse of Personal Information |
| G 0.39 Malware |
| G 0.40 Denial of Service |

| |
|---|
| G 0.42 Social Engineering |
| G 0.43 Attack with Specially Crafted Messages |
| G 0.44 Unauthorised Entry to Premises |
| G 0.45 Data Loss |
| G 0.46 Loss of Integrity of Sensitive Information |
| G 0.47 Harmful Side Effects of IT-Supported Attacks |
| IND.1.2 Insufficient integration of OT into the safety organisation |
| IND.1.3 Insufficient integration of OT into operational processes |
| IND.1.4 Insufficient physical access protection |
| IND.1.5 Unsecure project planning process/application development process |
| IND.1.6 Unsecure administration concept and remote administration |
| IND.1.7 Insufficient monitoring and detection procedures |
| IND.1.8 Insufficient test concept |
| IND.1.9 Insufficient life cycle concepts |
| IND.1.10 Insufficient security requirements for procurement |
| IND.1.11 Use of unsecure protocols |
| IND.1.12 Insecure configurations of components |
| IND.1.13 Dependencies of OT on IT networks |
| IND.2.1.2 Insufficient user and authorisation management |
| IND.2.1.3 Insufficient logging |
| IND.2.1.9 Manipulated firmware |
| IND.2.2.1 Incomplete documentation |
| IND.3.2.1 Incompletely documented remote maintenance access in the OT |
| IND.3.2.2 Insufficient availability due to dependencies on office and building IT |
| IND.3.2.3 Insufficient regulations for the use of OT remote maintenance access |
| IND.3.2.4 Insufficient human oversight over OT remote maintenance sessions |
| IND.3.2.5 Direct IP-based access to systems from insecure zones |

| |
|---|
| IND.3.2.6 Insecure alternative OT remote maintenance access in the event of faults |
| IND.3.2.7 Insecure design of OT remote maintenance accesses |
| IND.3.2.8 Outdated technical concepts for OT remote maintenance access |
| CON.1.1 Insufficient key management for encryption |
| CON.1.8 Compromise of cryptographic keys |
| CON.1.9 Forged certificates |
| CON.3.1 Missing data backup |
| CON.3.2 Missing recovery tests |
| OPS.1.1.3.5 Problems with the automated distribution of patches and changes |
| OPS.1.1.3.6 Insufficient recovery options for patch and change management |
| OPS.1.1.3.8 Manipulation of data and tools during patch and change management |